NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECURE INTEGRATION OF RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY INTO A SUPPLY CHAIN

by

Barry A. Craft Jr.

September 2005

Thesis Advisor: J.D. Fulp

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: **SECURE INTEGRATION OF RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY INTO A SUPPLY CHAIN**	**5. FUNDING NUMBERS**
6. AUTHOR(S)	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	**12b. DISTRIBUTION CODE**
Approved for public release; distribution unlimited	A

13. ABSTRACT (maximum 200 words)

Leveraging information to improve business practices is common throughout many agencies of the United States Government and the commercial world. Radio Frequency Identification (RFID) technology promises improved accuracy and time-saving in the area of inventory control/tracking. This report summarizes current RFID technology, including a Chapter dedicated to security; then offers several inventory-tracking implementations for a specific sponsor's environment.

14. SUBJECT TERMS RFID, Security, Supply Chain	**15. NUMBER OF PAGES** 113
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited

SECURE INTEGRATION OF RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY INTO A SUPPLY CHAIN

Barry A. Craft Jr.
Captain, Untied States Marine Corps
B.S., The Ohio State University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Author: Barry A. Craft Jr.

Approved by: J.D. Fulp
Thesis Advisor

Dr. Dan Boger
2nd Reader

Dr. Dan Boger
Chairman
Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Leveraging information to improve business practices is common throughout many agencies of the United States Government and the commercial world. Radio Frequency Identification (RFID) technology promises improved accuracy and time-saving in the area of inventory control/tracking. This report summarizes current RFID technology, including a chapter dedicated to security; then offers several inventory-tracking implementations for a specific sponsor’s environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Mr. JD Fulp for his mentorship and for fostering an environment of learning throughout the entire process. He has been a true leader and a gifted academic. I would also like to thank my wife who was supportive and understanding while I spent time numerous nights away from home conducting the research and writing this paper. Finally, I would like to thank the sponsors for giving me the opportunity to work with them. It has been a tremendous learning experience.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Radio Frequency Identification (RFID) is a term for a small, wireless radio system that uses emitted electromagnetic energy for the purposes of identification. In its present form, RFID systems consist of four different elements; a transponder (or tag), an interrogator (or reader), an antenna, and a host computer system that acts as both controller and database[1,2].

The basic system uses a reader that is networked to a host computer system to transmit an interrogation signal through an antenna to a target tag. The tag harnesses the electromagnetic energy and redirects a response through its own antenna back to the reader; thereby “identifying itself”. The reader then updates the database as to the presence of the tag in its area of coverage[3].

Modern RFID was first developed by scientists at Lawrence Livermore Laboratory when they realized that a receiver when stimulated by radio frequency (RF) power could respond with a coded signal. This system was connected to a computer database and used to control access to a nuclear weapons research facility[4]. The system became one of the first building entry control systems based on RF proximity detection.

Today, RFID is widely deployed in the United States. RFID is being utilized to collect tolls, unlock doors, secure library books and store merchandise, as well as to track palettes, boxes, and even individual items in a supply chain. Wal-Mart, Target, Metro and the Department of Defense (DoD) have lead the charge in implementing wide

scale RFID into their production, storage and other logistical processes[2]. The future utility of the technology is vast, and the potential benefits have not yet been fully realized.

B. MOTIVATION FOR RESEARCH

The sponsor of this thesis is interested in how RFID may benefit their production and warehouse facilities from both a supply chain and security standpoint.

C. CONTENT

Chapter II of this study explains current RFID technology, it capabilities, limitations, and functions. It is not limited to RFID in a supply chain environment, but object tracking and inventory are the major foci. Tags, readers, antennas, the basics of radio frequency communications, middleware and electronic product codes are all explored according to projected needs of the sponsor.

Chapter III presents logical models of the two different production lines and the warehouse facility of the sponsor. It concentrates on object state and the processes that move those objects into the new phase of production or storage.

Chapter IV integrates RFID into the models. In the case of the two productions facilities, the models demonstrate how RFID can be implanted into the line to better track objects for security and tracking purposes before they are moved to the warehouse. The sponsor is then given five different options as to how RFID can be integrated into its existing storage facility along with simplified cost equations that allow relative cost comparison among the presented options. The overall cost

and benefits of each of these options for the overall production facility is the focus of this Chapter.

Chapter V outlines the four major components of data security; confidentiality, availability, integrity and authenticity. Each element is defined and its value to the sponsor is quantified. Finally, the challenges and some solutions of RFID specific security are covered in some detail. This is an attempt to give the sponsor an idea of how RFID differs from traditional computer security and suggests some methods put forth by current research to overcome the many challenges that cost effective security present.

Chapter VI outlines the final conclusions of the research and gives recommendations of potential topics for further study.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PRESENT RFID TECHNOLOGY

In order for RFID technology to be useful, systems must be in place to read the data, track the objects and to leverage this capability to improve the manufacturing process. “The basic premise of RFID is that by attaching a radio frequency tag to an object, a computer can track that object without human intervention [1]”. This remote tracking allows a much higher level of automation, inventory control, and security throughout the key events in an object’s supply chain life span. This is where the most value is derived through the use of RFID.

A. TRANSPONDER (TAG)

A transponder, or tag, responds to the presence of a reader by transmitting its information when interrogated electromagnetically. The amount of information transmitted, the distances this information can travel, and the power source of the electromagnetic wave, differ widely from chip to chip depending on its application; but the basic premise remains. A tag is an object label that provides information to an observer. In its most basic implementation, an RFID tag serves as the rough equivalent of a license plate on an automobile. Figure 1 (below) illustrates the typical construction of an RFID tag. An antenna (RF radiator and collector) connected to a chip (processor and memory), both of which are mounted to some form of substrate material that facilitates their protection and mounting.

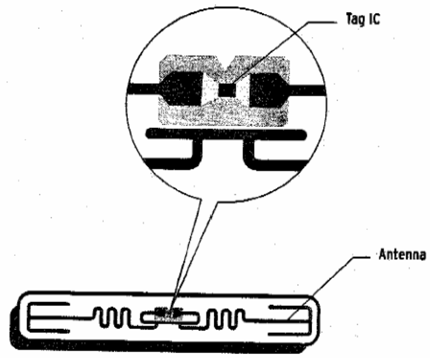

Figure 1. Tag Integrated Circuit and Antenna[1].

Tags come in a variety of different formats, the most basic of which is an electronic article surveillance (EAS) tag. With only 1 bit of memory, they simply signal their presence to the reader without any further identifying characteristics.

Perhaps one of the most distinguishing characteristics of a tag is its source of power. Passive tags have no onboard power source and are forced to harness the energy emitted by the reader. This is accomplished by capturing a portion of the incoming electromagnetic wave’s energy within the tag’s circuit; which generates sufficient onboard current to power a reply through its own antenna back to the reader.

Due to their lack of indigenous power, passive tags (as compared to active tags) have shorter ranges, but are cheaper to produce and more secure as they do not announce their presence unnecessarily. Passive tags are currently priced anywhere from $0.10 to $0.25 depending on the number ordered and its capabilities. The five cent tag is widely considered the cost point at which wide scale RFID

deployment will become economically feasible/justifiable [1]. However, this price point is largely dependent on costumer order volumes, market requirements, and production efficiencies [2]. Demand growth may remain slow until prices drop sufficiently; making the $0.05 tag largely a “catch-22” situation. Figure 2 illustrates the classic supply-vs-demand relationship.

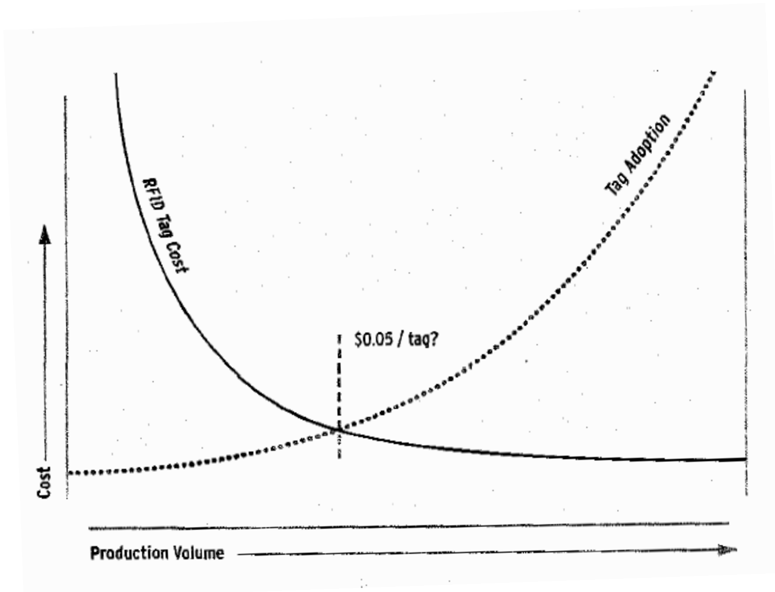

Figure 2. Tag Cost vs Production Volume [1].

In contrast, an active tag has its own power source with which to respond to a reader interrogation. These tags can transmit up to the distance of a football field[2]; have higher degrees of accuracy, the possibility of more complex information exchanges, and the capability to include their own microprocessors[3]. Due to the presence of a battery, active tags have the positive characteristic that they do not require the imparted RF energy of a reader to respond, but have the negative characteristic of a finite lifespan. The typical usage of active tags is to track high value assets from long distances where the price

of the tag is insignificant in comparison to the value of the article tracked.

Another class of tag that is growing in popularity is the semi-active (or semi-passive depending on the manufacturer) tag. Like a passive tag, this hybrid is also small, lightweight and has a limited memory/processor. It relies on imparted RF energy to respond to interrogations by the reader. However, unlike its passive cousin, a semi-active tag also draws on power from an internal battery to perform tasks such as operating an onboard microprocessor and possibly to increase the power of its response transmission[2]. It is less expensive, but like a fully active tag also has a finite life span.

The type of memory a tag employs is another important tag characteristic. Beyond the basic EAS (1 bit), tag memory varies from sixteen to several hundred kilobits[2]. The amount and type of memory, the power source and overall capability of a tag is largely dependent on the application and has a great impact on cost.

The most basic form of tag memory is read only (RO), in which the memory is permanently written by the manufacturer. For this reason RO tags are usually the least expensive (not needing to support write or re-write functionality) and most secure since unauthorized re-writes are impossible[4].

A similar but distinctly different type of memory is a WORM or Write Once Read Many. Like RO, the tag can be programmed only once; however, this write can be done at the customer level (i.e., “after market”) thus offering more flexibility at the expense of increased cost.

Higher end tags have read/write (RW) memory in which a tag may be read from or written to an unlimited number of times. This type of tag offers the greatest flexibility and functionality but at a higher cost. In the case of tags with writeable memory, the read range is far greater than its write (or programming) range, requiring the write process to be more deliberate in nature.

Special tag classes have been developed that follow the Electronic Product Code (EPC) standard, which will be covered in more detail later in the Chapter. These tag classes are explained in Table 1 below.

EPC Device Class	Definition	Programming
Class 0	"Read only" passive tags (RO)	Programmed by manufacturer
Class 1	"Write-once, read-many" passive tags (WORM)	Programmed by costumer
Class 2	Re-writable passive tags (RW)	Reprogrammable
Class 3	Semi-active tags	Reprogrammable
Class 4	Active tags	Reprogrammable
Class 5	Readers	Reprogrammable

Table 1. EPC Tag Classes[3].

Table 2 summarizes the advantages, disadvantages and applications of each type of tag.

Tag Type	Advantages	Disadvantages	Application
Active	Greatest read range, memory capacity, continuous signal	Batteries, requires maintenance, larger in size	Used for high value asset tracking

Semi-Passive	Greater read, longer battery life, IC capability	Finite battery life, more expensive than passive tags	Reusable containers and medium value asset tracking
Passive RW	Long life, multiple form factors, erasable and reprogrammable memory	Time and expense to program	Case and pallet applications
Passive WORM	Well suited for individual item identification, Memory controlled at manufacturing stage	Limited to a few re-writes replacing existing data with new data, Memory controlled at manufacturing stage	Case and pallet applications
Passive RO	Simplest and cheapest approach	Identification information only, no tracking or memory updates	Case and pallet applications

Table 2. RFID Tag Characteristics[1].

Table 3 suggests some considerations when selecting an RFID tag for supply chain use.

Consideration	Comments
Tag Placement	Read rate is affected by the orientation of the tag on the box or pallet relative to the reader.
Size and Form factor	Individual containers often have a pre-designed area for tag placement which could restrict size and placement.
Read Speed	The time required for a reader to accurately read the ID number from a tag. Faster read speeds permit faster conveyance of tagged items through a readers RF field-of-view.

Read Redundancy	The number of times that a tag can be read while it is within a readable area. Often a tag must be read up to three times before its data will be captured without error[2].
Data Requirements	The amount and type of data a tag contains. A function on its application.
RF Interference	Read rates and error rates will be affected by ambient RF noise and proximity to other tags and readers.
Read Range	Range requirements will largely determine which RFID technology (frequency, class, active vs passive, memory type, etc.) is chosen.
Security	Some applications of RFID may require confidentiality and/or proof of authenticity as security measures.

Table 3. Tag Selection Considerations[2].

RFID Tag suppliers include:

Alien Technology – http://www.alientechnology.com

Avery Dennison – http://www.averydennison.com

Impinji – http://www.impinj.com

Matrics Systems Corporation – http://www.matrics.com

Philips – http://www.semiconductors.philips.com

Rafsec – http://www.refsec.com

Texas Instruments – http://www.ti-rfid.com

B. INTERROGATOR (READER)

Along with the transponder tag, an interrogator (or reader) is a critical component of an RFID system. They

capture and process tag data and communicate with the computer that hosts the appropriate RFID middleware. Some readers are capable of writing data to a tag while others simply collect reflected energy (i.e., read tags). When readers read information from a tag, it uses one of two basic ways: inductive coupling or backscatter radiation. Either of these RF techniques serves to “energize” the tag.

Tags designed to work with inductive coupling—aka “transformer” coupling due to usage of the same principle that allows the primary and secondary coils in a transformer to couple energy--typically reply with their ID numbers by load-modulating the coupled RF energy with their ID numbers. For example; a logical ‘0’ is communicated to the reader via a low load, and thus low energy coupling, while a logical ‘1’ is communicated to the reader via a high load, and thus high energy coupling.

Tags designed to work with backscatter radiation typically reply with their ID numbers by modulating their RF reflective cross-sections with their ID numbers. For example; a logical ‘0’ is communicated to the reader by the tag reducing its reflectivity, while a logical ‘1’ is communicated to the reader by the tag increasing its reflectivity. Note that backscatter communication has its roots in basic radar (RF echo-reply) theory. Figure 3 illustrates the basic reader-stimulus and tag-response concept underlying RFID tag reading regardless of the specific RF technology used.

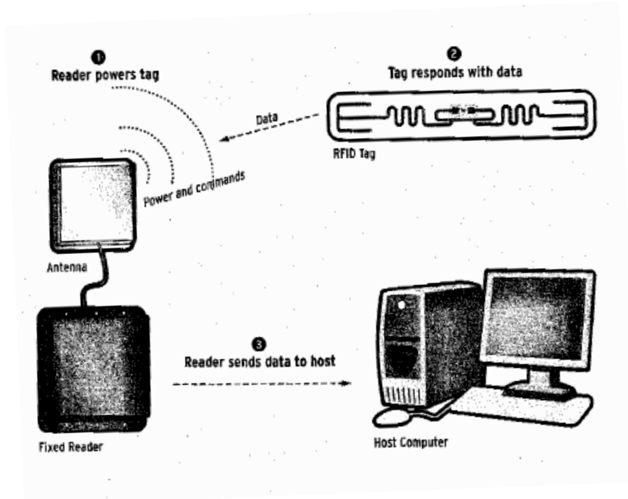

Figure 3. Tag-Read-Host Communication[1].

The range of the response is largely a function of: reader radiated power, operating frequency, antenna design, antenna orientation, ambient RF interference, and the proximity of RF absorbing and scattering substances. The size of both the transmitter and receive antenna is application dependent but the power of the transmitter is limited by Federal Communication Commission (FCC) regulations or other regulatory bodies outside the United States.

Because there may be many tags in the vicinity of the reader when the interrogation signal is transmitted, a reader must also be able to receive and manage multiple replies at once, sometimes as many as hundreds per second[2]. This is accomplished through collision avoidance algorithms that are often closely guarded proprietary secrets due to the competitive advantages they give their respective manufacturers.

Collision avoidance is achieved in its most simple incarnation by requiring each tag to wait a random amount of time before responding. This delay, also known as

backoff, is a critical component in the IEEE 802.3 CSMA/CD--and closely aligned Ethernet--LAN protocol. If the collision avoidance technique introduced by the Slotted ALOHA protocol; wherein stations (tags) may only begin transmission at coordinated start (slot) times, is added to the backoff technique, then a further enhanced avoidance protocol emerges: along with its concomitant complexity costs. Other, more complex, avoidance algorithms include reduction through binary search trees; or in the case where a apriori knowledge is available, code division multiple access (CDMA).

When comparing these three basic techniques (slotted-backoff, binary search, and CDMA) we see the typical technology tradeoffs at play. An oversimplified explanation proceeds thusly. Pure backoff is simple to implement (each tag generates a random wait value). Adding “slots” to backoff entails some means of synchronizing all tags in a reader’s range, thus adding complexity but decreasing the chances of overlap type collisions vice start-of-transmission type collisions. Regardless of how efficient the slotted-backoff technique gets, it will always remain non-deterministic (roll of dice) in the time taken to read all tags in a reader’s range.

Binary search methods; wherein statistically half of all tags are temporarily silenced after each collision, is deterministic in behavior at the cost of more sophisticated (and costly) readers and tags. CDMA methods; wherein tags employ the same CDMA “chipping” techniques used by some in the cell phone industry, can be extremely fast, but require that each tag be designed at the time of manufacture to “chip” its ID number. Given the EPC proposed RFID number space of 96 bits, this would necessitate that EVERY chip

intended for global interoperability would need to be of globally-unique design.

There a several types of readers from a number of companies. Most are developed specifically for supply chain RFID applications. Some reader types include; handheld, mobile mounted, fixed and combination reader/writer[2] (see Figures 4, 5, and 6). In a typical production facility tracking setup, readers are configured to read any set of tags that pass through their read area. These areas are typically referred to as portals. Portals are located at critical locations (e.g., phases, processes or product “milestones”) in the production or logistical chain where these product “events” can be tracked and counted to ensure an accurate inventory and provide the manufacturer with much enhanced production/product “awareness”.

Figure 4. Handheld Reader.

Figure 5. Fixed Station Reader.

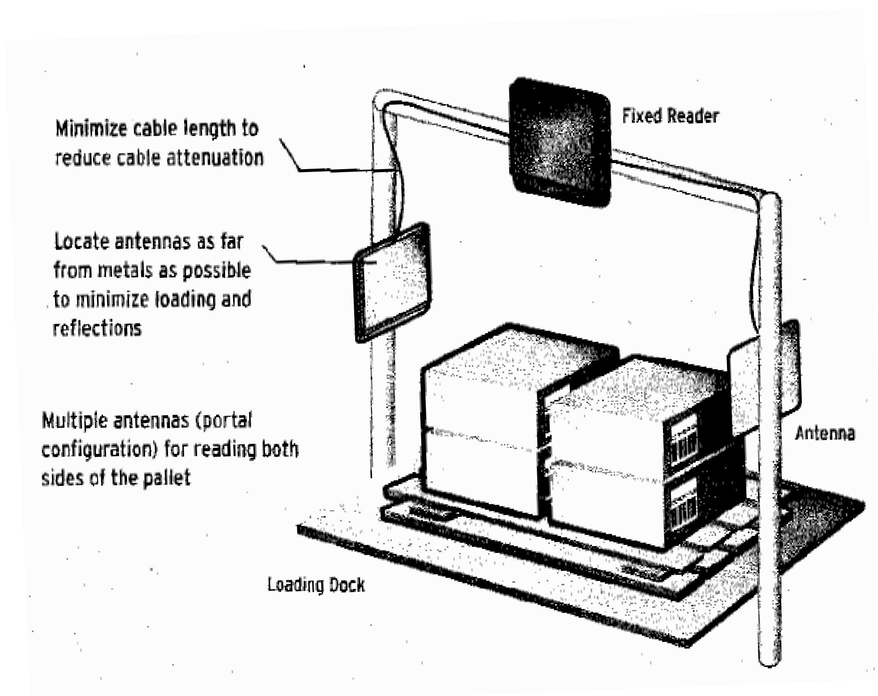

Figure 6. Archway Portal Reader[1].

Sufficient understanding of RFID technologies that relate to the all-important read range requires some elaboration on the basic air interface technologies

(induction and backscatter) discussed earlier. Readers can use either magnetic (aka induction or “near-field”) or electromagnetic (aka backscatter or “far-field”) energy forms to excite a transponder.

Inductive systems are used in short range (on the order of 10cm) situations where a tag is expected to pass directly through a specific area that is in close proximity to the radiating reader’s RF energy. If the RFID application is amenable to such short range operation (e.g., reading an individual passport at a customs booth) then many benefits result. For one, such close range interrogation implies a 1:1 reader:tag situation; obviating the troublesome collision problem. The close range also reduces the potential deleterious impact of ambient RF interference. And the security/privacy implications are rather obvious for situations where the information provided by the tag is somehow regarded as sensitive. However, the use of near field induction systems also results in a shorter range system. Personnel identification systems found in secure areas, checkout systems at libraries, and theft prevention systems found in retail stores are example applications for this relatively short range RFID technology. Low frequency (LF) and high frequency (HF) systems, described in a later section, use near field RFID.

Outside of the near field, the radiation field, or far field, excites the circuit in the tag. Far field antennas are shaped differently than those intended to operate in an inductive environment. When a tag is exposed to a field generated by the reader, the tag absorbs sufficient RF energy to power its chip as it modulates it reflective cross-section as a reply back to the reader’s receiver.

For maximum performance, both the tag and reader antenna are coupled at the same frequency and as a result, frequency of operation has perhaps the largest impact on RFID system performance. The frequency in which the RFID system operates directly impacts data transfer rate foremost; the lower the frequency, the lower the theoretical maximum rate of data transfer. However, other factors have a large impact on frequency selection. These include antenna size, interference from outside sources, electromagnetic bleed and range. The radio frequency spectrum is shown in figure 7 below.

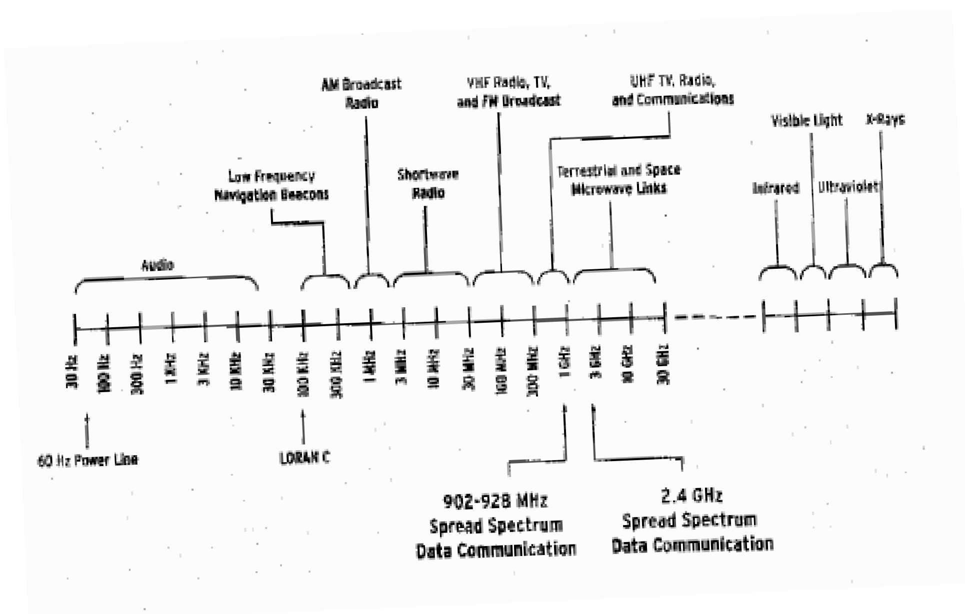

Figure 7.   RF Electromagnetic Spectrum[1].

C. ANTENNA

The size of the transmitting and receiving antenna is largely a function of the frequency of transmission. Since the function of the RFID antenna is to transmit and receive electromagnetic (EM) radio waves, the antenna design must be optimized for the particular frequency, polarity, and

directionality desired. As stated before, the antenna’s function is to transmit and collect RF energy to transfer power and/or data between readers and tags. This process demands that the antenna be specifically scaled for optimal performance.

The most basic antenna is a half wave dipole which is similar to a standard automobile antenna.

The equation

$$\lambda = \frac{c}{f}$$

where λ is wavelength, c is speed of light in a vacuum and f is frequency, describes the fixed relationship among these three RF characteristics. When a dipole antenna is approximately one half wavelength long the capacitive and inductive reactances are equal and cancel as a result. In this condition, the antenna is in resonance and will maximize performance. As an example; for an operating frequency of 915 MHz, an optimized antenna would be approximately 6 inches in length. This relationship between antenna length and operating frequency takes on increased importance given the desirable RFID goal of minimizing tag size/footprint.

Another critical factor in antenna performance is polarization. EM waves traveling in free space have an electric field component (E field), and a magnetic field component (H field) which travel perpendicular to each other and perpendicular to the direction of radiation propagation. The orientation of the E vector is used to define the polarization of the wave. If the E field is orientated vertically, the wave is vertically polarized. Linearly polarized systems have longer read ranges when the

tag is optimally orientated. As a result, this polarization is best when the tag orientation is known and fixed.

In a linear polarized antenna, radiation travels in a linear pattern at depicted in Figure 8.

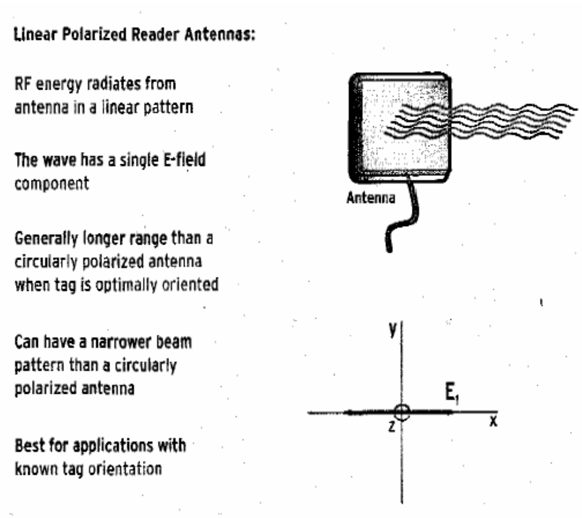

Figure 8. Linear Polarized Antenna[1].

If, however, the E field rotates, it is circularly polarized. A circular polarized antenna radiates energy in a circular pattern. This system is designed to increase signal reception in the presence of multipath, scattering, or situations that may result in non-optimal reader-to-tag antenna orientations[1] (e.g., both reader and tag have vertically polarized antennas but the tag’s antenna is rotated some angle--90 degrees representing the worst case--with respect to the readers antenna’s orientation). Circular polarized antennas are less sensitive to tag orientation but at the cost of decreased maximum theoretical read range. . Figure 9 provides a basic illustration.

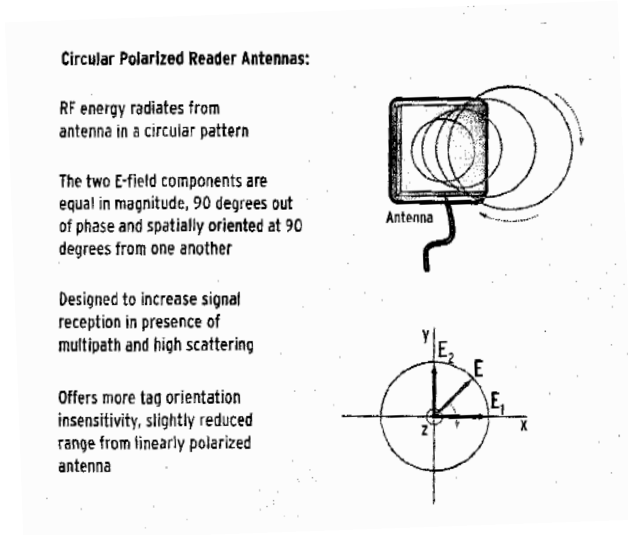

Figure 9. Circular Polarized Antenna[1].

Radio frequency waves are tightly controlled by the FCC and other regulatory bodies internationally. As a result, RFID systems fit into one of four frequency ranges; low-frequency (LF), high-frequency (HF), ultrahigh-frequency (UHF), and microwave. Because radio waves behave differently and have varying capabilities and limitations depending on their frequency, frequency selection is highly application dependent [4].

Key factors involved in the selection of the frequency band for a specific application include; read range, accuracy, data speed and the material composition of the objects the tags are affixed to[2]. A microwave system (nominally ~2.4GHz) provides for longer read ranges and higher potential bandwidth but its performance is largely degraded in the presence of liquids and metals.

In contrast, an LF system (nominally 100-500 KHz) is better able to penetrate liquids and not be adversely refracted and reflected by metals. LF systems have been in use since the 1980’s. This longer history with respect to the higher frequency systems, in addition to on the use of

the tighter-coupled near field technology, results in relatively high accuracy rates. Because of its low frequency nature, it suffers less of the prevalent HF- and UHF-based electromagnetic interference. Typical LF applications include; access control, payment technologies, animal identification, and vehicle key locks.

HF systems also rely on near field coupling for data transfer. The dominant implementations today operate at 13.56 MHz and have a slightly higher data transfer rate than LF systems. Read ranges are typically several inches extending to a foot in some cases with the primary applications including; access control, electronic article surveillance, payment cards, anti-counterfeiting, personnel identification, pharmaceuticals and chemical products.

UHF systems operate in the 902 to 928 MHz band in the United States. FCC regulations limit unlicensed transmissions in this band to no more than four watts of power. This band is shared by many commercial applications and interference from outside sources is of concern is some instances. UHF RFID systems have a read range of over twenty feet[1] and are capable of much higher data transfer rates than LF and HF systems. However, because of its shorter wavelength, UHF energy is attenuated more readily in the presence of water/moisture. Thus attempting to employ UHF tags on liquid products may prove untenable. Typical applications include; supply chain, baggage control, toll collection, asset management, and industrial automation.

Microwave RFID systems operate in the 2.4 to 2.48 GHz range. Due to this relatively high frequency, data transfer is faster than that of any of the other frequencies employed in RFID. Read ranges vary from three to ten

feet[1]. Typical applications include item tracking and toll collection.

Table 4 suggests some considerations when selecting a frequency for an RFID system.

Band	Frequency Range	Read Range	Applications
Low Frequency (LF)	100-500 KHz	Inches	Access Control, Animal Identification, Vehicle key locks, card payment technologies
High Frequency (HF)	13.56 MHz	Up to 3 feet	Access Control, Smart Cards, libraries, electronic article surveillance, Pharmaceuticals, liquid products
Ultra High Frequency (UHF)	866-956 MHz	Up to 20 feet	Supply Chain use, Baggage handling, inventory control and warehouse, asset tracking management, toll collection,
Microwave	2.4-2.48 GHz	Up to 10 feet	Asset tracking, toll collection, Industrial Automation

Table 4. Frequency Characteristics[1].

D. MIDDLEWARE

The individual components of an RFID system are dependent on the presence of a solid network where the readers are able to acquire information from the tags, and then communicate this information to a central “host”

system where value-added processing can take otherwise useless tag ID numbers and use them to point to a more informative database entry that tracks the associated tagged item over its lifespan. The host computer running the RFID system is dependent, in general, on the RFID software, aka “middleware”, it runs. Therefore the computer itself is of less interest than the middleware. This purpose-built for RFID software is leveraged by the RFID user to manage the data collected by the RFID readers.

Middleware facilitates the communication with the many nodes (readers) in the RFID network. It provides the interface between the hardware and the incoming data and keeps a record of the transactions it observes. The primary elements of the RFID middleware are; reader device management, data management, and application integration[5].

Software is involved in every part of the RFID system, from the individual tags and readers, to the coordinating middleware and the host system’s operating system. It facilitates the basic interaction between the tag and the reader, and interprets the raw data delivered by the readers in the context of the larger system being modeled; e.g., a retailer’s inventory database, a facility’s access-control system, or user account information for the purchase of gasoline. In short, software is the “glue” that binds all the disparate parts into a functioning whole, and the RFID middleware, is that subset of the software that deals with the RFID-specific portion of that whole.

Software also provides anti-collision solutions when multiple tags are present in the response zone interrogated by the reader. This allows the reader to distinguish between individual tags if and when their responses would

otherwise overlap and interfere with reliable reads. These algorithms are complex, varied and proprietary. Commercial vendors provide “out of the box” solutions, but choosing the correct vendor according to system requirements is a critical decision point.

Software provides other services such as error detection and correction as well as encryption, authorization and authentication. Specific security aspects of RFID, both from a hardware and software standpoint, will be discussed in detail in a later Chapter.

E. ELECTRONIC PRODUCT CODE (EPC)

The most common implementation of a supply chain RFID system utilizes the electronic product code standard (EPC) organized and managed by EPCglobal[1]. The following section will describe the key components of the standard and the most common form of integration into an RFID supply chain network.

EPC is simply a hierarchical numbering system that allows the assignment of a unique identifier to each article to be tracked in a supply chain. It is intended to replace the Universal Product Code (UPC) which is in use today for non-RFID object tracking. The current format is depicted in Figure 10. A brief explanation of each major field in the header follows:

- Header – two digit code identifying the EPC version number
- EPC Manager – seven digit code identifying the enterprise using the EPC code
- Object Class – six digit code signifying the product category

* Serial Number – nine digit code identifying the unique article within the hierarchy

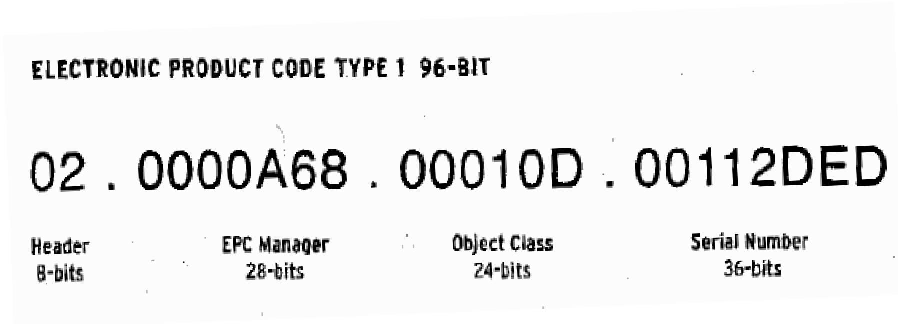

Figure 10. Electronic Product Code Format[1].

Since each digit is a hexadecimal number--having sixteen different values, 0 through F--an EPC code is a 96-bit unique identifier capable of 16 million object classes with 68 billion serial numbers in each class.

Since the late 1970’s, UPC product tracking in the form of bar codes has been the standard for automated information retrieval for UPC marked products[1]. Though the barcode/UPC system is effective, it has several limitations that RFID/EPC system addresses. The germane attributes to consider when comparing RFID/EPC and a standard barcode/UPC scanning system are; read method, read speed, read accuracy/reliability, label durability, data storage capacity, flexibility of information, costs, and security.

Read Method – While bar code optical scanners provide absolute visual (or auditory) verification of a successful read of the single, specific item under the reader’s attention immediately, an RFID/EPC system may not provide such surety regarding which item was read, owing to the general difference in technology employed by each. Barcode systems utilize a highly directional

light beam that must be directed upon one specific item at a time. RFID systems, on the other hand, utilize an omni- or semi-directional RF beam pattern to read whatever item(s) may be in its range. The implication is that a successful RFID read may not indicate either a precise item, or a precise physical location for an item; as is the case with a bar code read. This difference is analogous to the comparison of sight and hearing as depicted in Figure 11.

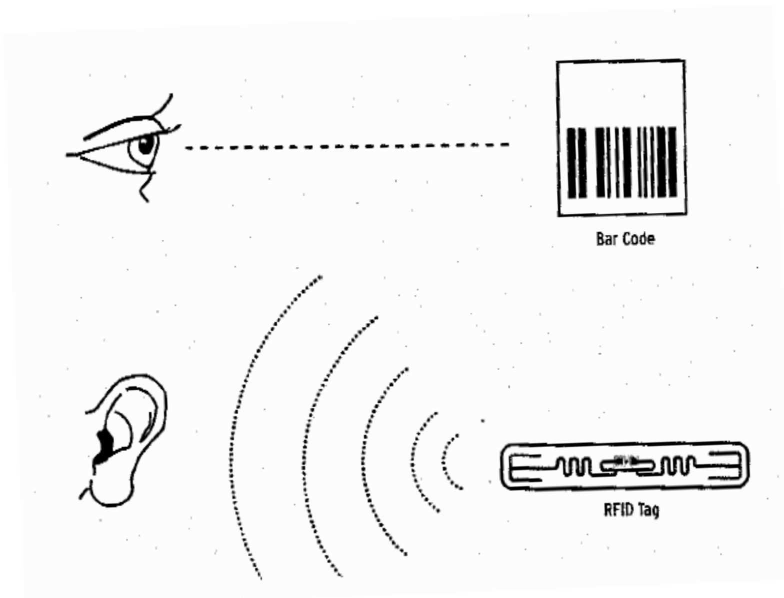

Figure 11. Line of Sight vs RFID [1].

Read Speed – Even under the best of circumstances, RFID tags can be read far more rapidly than bar codes can be scanned. This RFID advantage offers great value where large volumes of items are being tracked. Figure 12 below demonstrates the relative read speeds of RFID systems and bar code scanners.

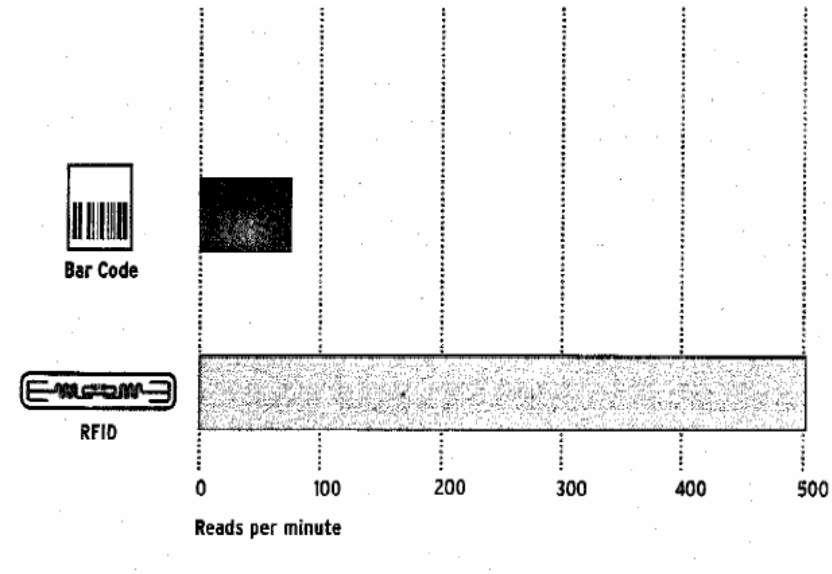

Figure 12. Bar code vs RFID[1].

Read Accuracy/Reliability– Automated bar code scanners provide for read accuracy rates approaching 100%. A 100% accuracy rate with only one RFID scan is not a trivial endeavor, but as systems and processes improve, RFID systems should quickly achieve this standard[1].

Durability – To protect them RFID tags are typically encased in a protective coating, making them far more durable than bar code labels[1]. However, both rely on the some sort of adhesive to attach them to the item. The most vulnerable portion of an RFID tag is the point at which the antenna is attached to the circuit[4]. If this connection is severed, the chip will be effectively disabled. Barcodes, on the other hand, have the disadvantage of being rendered inoperable if they become sufficiently marred or otherwise obscured.

Data Storage Capacity – Unlike EPC which is capable of identifying items down to a unique, individual article through its large 96 bit serial number UPC is used to identify an item’s classification level only[1]. Though some 2D UPC numbers may contain as many as a thousand characters, RFID tags may contain several kilobits of information which can include several thousand characters[1]. This allows a greater number of product characteristics to be tracked; such as date of manufacture, time spent in transit, expiration date and date of last service.

Flexibility of information – RFID tags are capable of supporting both read AND write operations, enabling information updates in real time. Bar codes must be physically replaced if a modification/change is required.

Cost – RFID systems require a substantial up front investment of capital for procurement and operating costs. A Return on Investment (ROI) cost calculation may provide information as to the future savings RFID will provide.

Security – RFID tags are continually expanding their ability to protect the confidentiality, authenticity and integrity of the information they contain and provide. Currently, most RFID tags lack the memory and logic resources necessary to provide security mechanisms. A general discussion of security and the on going research into RFID specific features and protocols will be covered in Chapter 5. In general RFID tags pose

additional security threats in which bar codes are not subject to. For example, to read a bar code, an observer mush have physical access to the label, position it in the line of sight of the reader and understand the information that is scanned. In contrast, an RFID system without security features installed will answer any interrogation within it communication range. No physical access or line of sight is required.

In order to manage the EPC system, EPCglobal has developed the following middleware schemes to collect, process, filter and aggregate EPC data.

The Object Name Service (ONS) matches EPC object information to the information stored about the product; much like a Domain Name Server (DNS) maps website names to Internet Protocol (IP) addresses on the Internet. When the middleware receives an EPC serial number, it queries an ONS server which will “point” the middleware to a database where more detailed information about the product is located. The system is highly scalable and reliable.

An EPC Information Service (EPCIS) specifies the service and interfaces necessary to facilitate the data exchange between the applications across the entire supply chain. A central repository facilitates data sharing and updating, ensuring that true end-to-end supply chain integration is possible.

III. PRODUCTION FACILITY MODEL

A. INTRODUCTION

The purpose of this Chapter is to outline each of sponsor's production and the warehouse facilities in a logical fashion. The desire is to quantify each process in order to identify the critical stages where improved tracking and control measures can be leveraged to enhance the sponsors overall supply chain.

A state transition diagram graphically represents the status of an object in a given context, the events that cause a transition from one state to another, and the actions that result. Modeling a facility along the lines of such a diagram not only serves to abstract out RFID-relevant processes from the myriad non-relevant processes, but it also presents a simplified model from which the reader can quantify the logical process that a product undergoes from its genesis to the time it leaves the facility.

Each diagram is intended to identify the significant (think RFID-relevant) transitions from one given state to the next in each phase of the product life cycle. Though, in reality, each product may not undergo each and every transition included in the diagram, it is assumed for the purposes of this study that all products follow the entire linear process outlined. This decision was made in order to avoid confusing decision points which ultimately have no significant affect on the overall processes nor on the recommendations made in Chapter VI.

B. PRINTING AND BINDING FACILITY DIAGRAM

The following diagram outlines the logical printing process from state to state with each transition explained where necessary. Though not every detail of the process is displayed, a broad overview that captures the events significant to this study is encapsulated. The reader is assumed to have a apriori understanding of each of the existing processes. The goal of the diagrams is to simply develop a common understanding that can used to compare and contrast future recommendations and quantify changes to each process with future diagrams.

Each object state and transition will be labeled with the following notation:

State Printing (SP) – State of a product during the printing phase of the production process. Each state is given a title and labeled in a logical, numerical sequence from 1 to n.

Transition Printing (TP) – Transitions of a product from the one state to the next in the printing process. Each is given a title describing the transition and labeled in a logical, numerical sequence from 1 to n.

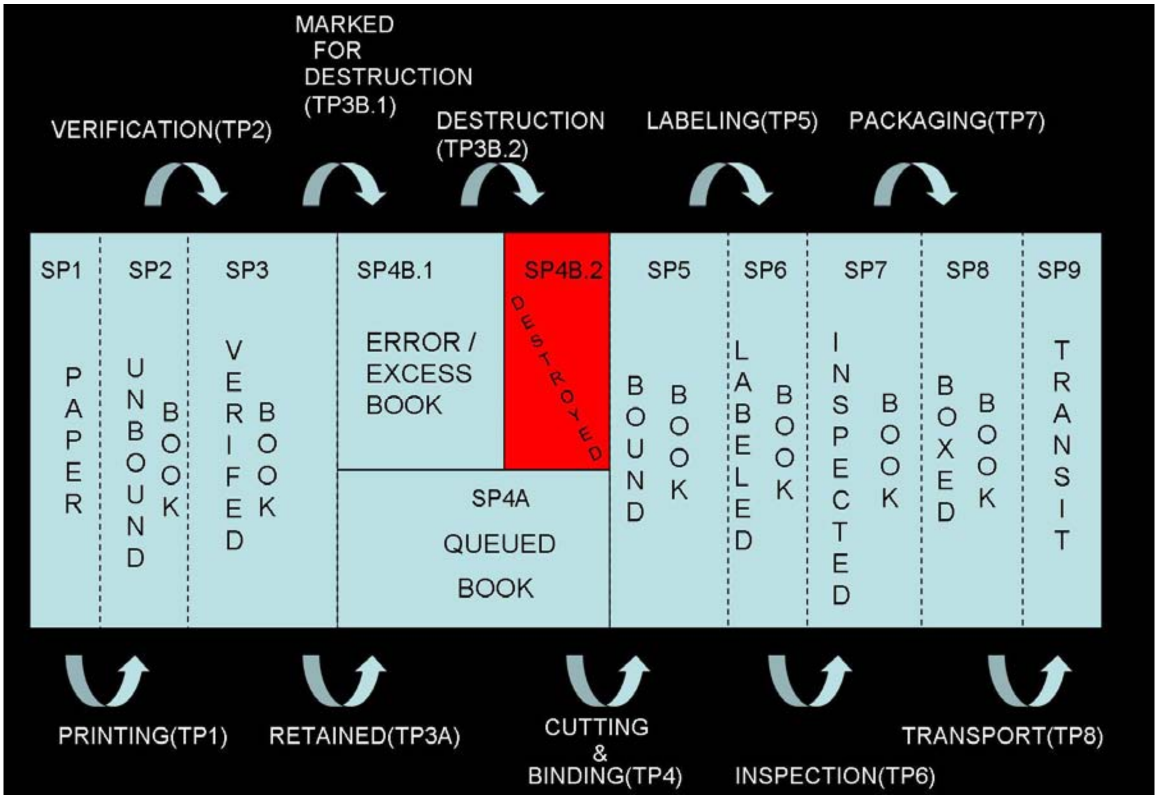

Figure 13. Printing Process Diagram.

The diagram demonstrates the transition that blank paper undergoes while it is transformed into a sensitive/controlled object. Objects not destroyed during the disposal phase continue to the warehouse phase outlined later in the Chapter.

The areas of significance in the printing process are; when the book is labeled, how disposed books are tracked and recorded, and the way in which the books are loaded into their individual boxes.

Books are currently labeled and entered into the production facility database during the “labeling” phase making it impossible to track the location or whereabouts of a potential sensitive object until well into the production process. Books that are marked for disposal are

not kept under positive control through a labeling or tracking system.

Though objects may remain in the production phase for several weeks, it is currently difficult for the facility manager to locate a specific object in the process or conduct a product inventory without hand reading each labeled item in the facility. Unlabeled items can only be tracked using visual confirmation of its presence. This is both time consuming and manpower intensive.

C. TAPE PRODUCTION FACILITY DIAGRAM

Much like the printing process, the tape production diagram outlines the manner in which raw tape in punched, loaded into canisters, labeled and packaged for shipment to the warehouse facility. Each object state and transition will be labeled with the following notation:

State Tape (ST) – State of a product during the each phase of the punching and loading process. Each state is given a title and labeled in a logical, numerical sequence from 1 to n.

Transition Tape (TT) – Transitions of a product from the one state to the next in the punching and loading process. Each is given a title describing the transition and labeled in a logical, numerical sequence from 1 to n.

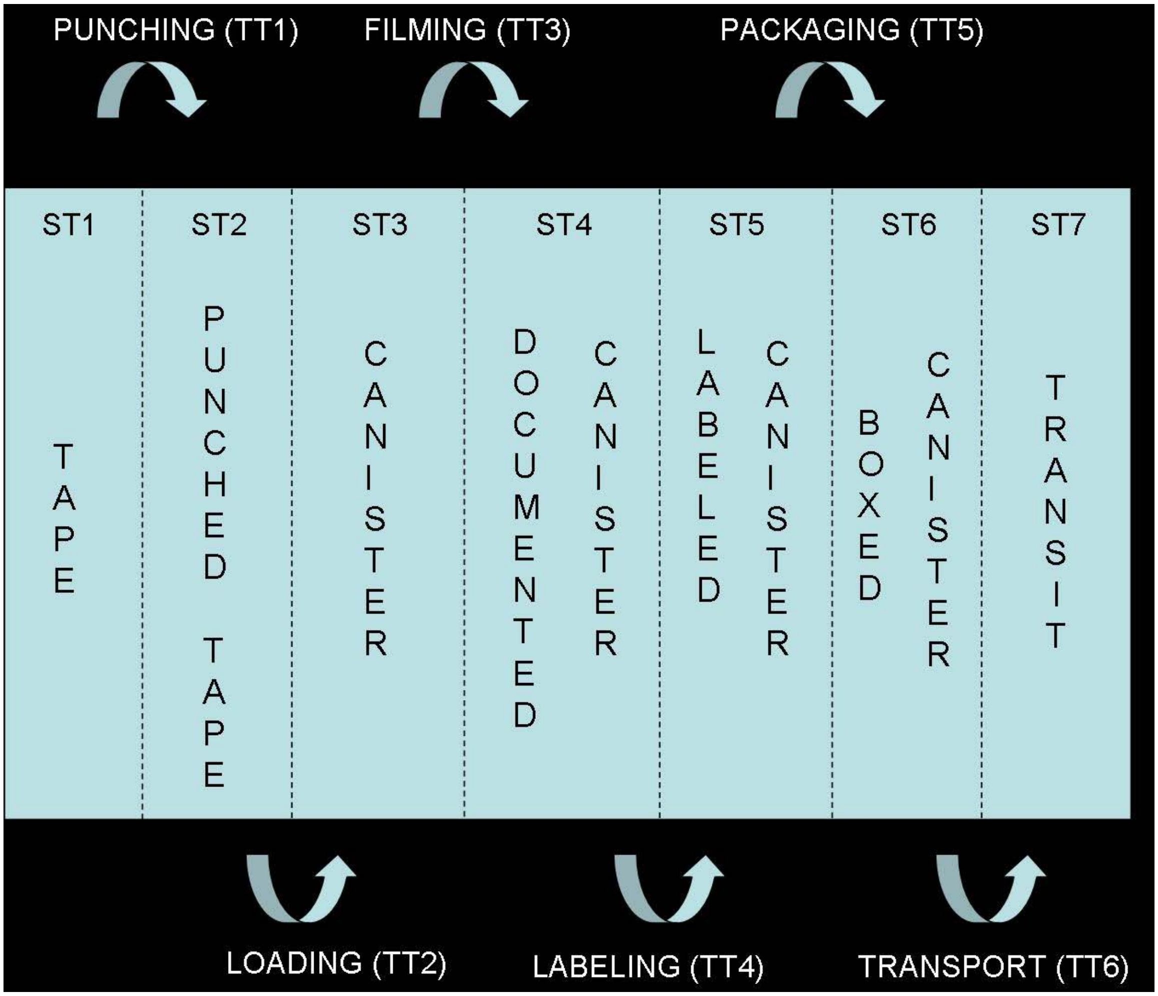

Figure 14. Punching Process Diagram.

Of significance during the tape production process is the stage in which the labels are transferred to the canisters and read into the production facility database.

Unlike the printing process, tape production occurs in a much more compact and easily defined setting. Few if any extra materials are created and errors are infrequent. This makes it much easier for the facility manager to track specific products and conduct an inventory. Labeling occurs early in the process and canisters transition from creation to the warehouse in a much smaller period of time. All

these characteristics contribute to an environment where more positive control can be maintained.

D. WAREHOUSE FACILITY DIAGRAM

The warehouse facility diagram outlines the final process a product goes through before shipping to the customer. During this phase, every product is assumed to reside in the facility long enough to undergo the inventory process, although in reality it is possible that some products may arrive and be distributed before a bi-annual inventory occurs.

Other significant phases include the collection and inspection processes. Each object state and transition will be labeled with the following notation:

State Warehouse (SW) – State of a product during the each phase of the storage and distribution process. Each state is given a title and labeled in a logical, numerical sequence from 1 to n.

Transition Warehouse (TW) – Transitions of a product from the one state to the next in the storage and distribution process. Each is given a title describing the transition and labeled in a logical, numerical sequence from 1 to n.

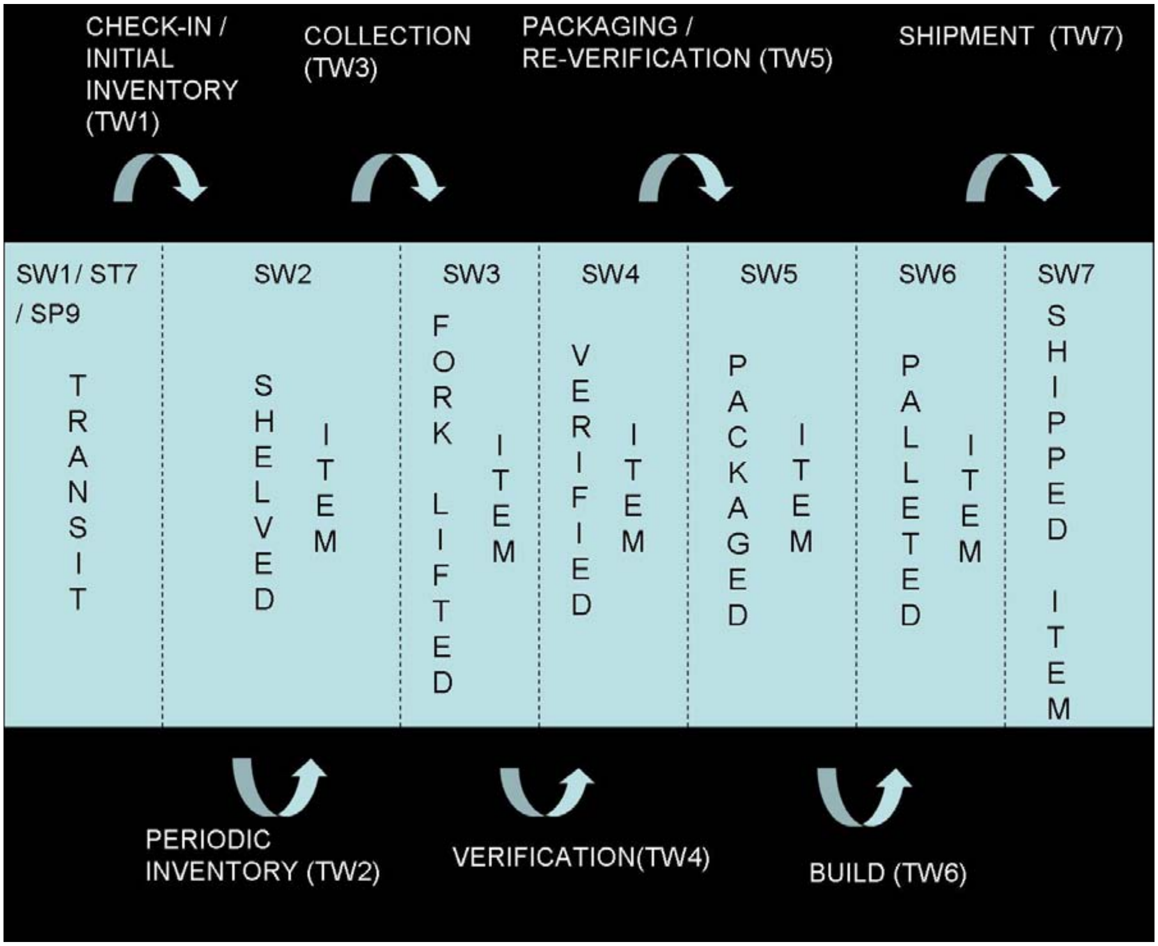

Figure 15. Warehouse Process Diagram.

E. SUPPLY CHAIN OVERVIEW

The complete supply chain model demonstrates how a raw material undergoes several state transitions before it is moved to the warehouse facility and finally shipped to the customer. Currently, object tracking begins during the labeling process of the printing and tape production phases and relies on bar code scanners and a manpower intensive and time consuming inventory process. The managers of each facility are unable to easily locate or track a specific object with an automated process.

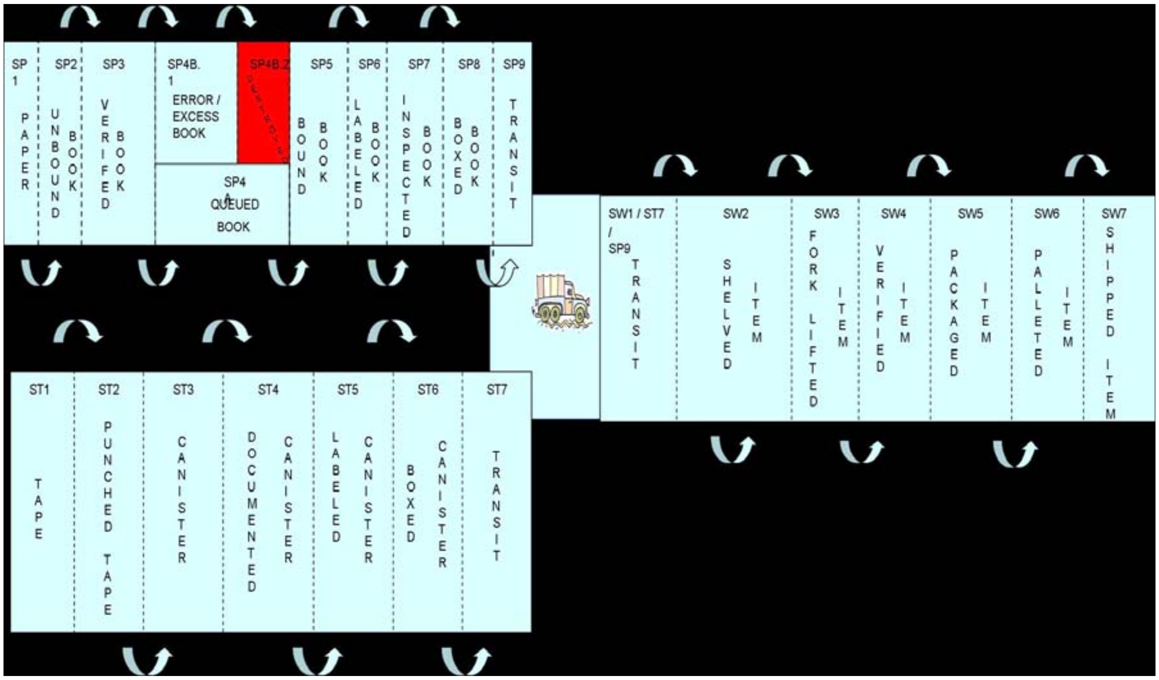

Figure 16. Supply Chain Diagram.

F. CONCLUSIONS AND RECOMMENDATIONS

Currently, books are labeled too late in the printing process to ensure a positive chain of custody throughout the production phase. Labeling should occur immediately after the object becomes sensitive which occurs after verification. Further, due to the physical layout of the printing facility, it is necessary to have an automated system to track the status and location of each of these entities during the production process. This will allow the facility manager to immediately locate an object on the production floor or read its status.

Though an automated process will add only marginal value to the tape production process, value will be added later in the supply chain making inventory and tracking of canisters much faster and easier. As a result, the current

labeling process should be replaced with a more useful, automation-friendly (RFID) system.

During the warehousing stage of the supply chain, inventory is currently conducted bi-annually by hand with the necessity for each item to be visually inspected and marked as present. This means that it is possible for an item to be missing for up to six months before its absence is detected, presenting clear security implications. Inventory should occur far more frequently.

In addition to the time-consuming inventory process, it is also currently necessary for each item to be identified and then checked two separate times in two separate locations before packaging and shipment.

An automated process would allow inventory at much more frequent intervals giving the facility manager confidence in the whereabouts and status of each of the sensitive items in his or her care. This inventory would occur through all phases of the warehouse process, from the time of introduction into storage until shipment; making it unnecessary for two separate verifications during collections phase and eliminating the manpower and space these processes use.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RFID INTEGRATION INTO THE PRODUCTION FACILITY

A. INTRODUCTION

The strength of RFID is the ability to identify the presence of an object in an automated fashion, requiring little or no human input. This knowledge can be leveraged to ensure that a product is not misplaced or improperly removed from the supply chain.

As stated previously, it is not necessary for the object to be in the line of sight of its reader; making large scale and frequent inquiries to update object status and location possible. In this Chapter, state transition diagrams are again used to demonstrate how RFID could be integrated into all three phases of the supply chain to better track product location and status, as well as to facilitate more frequent and rapid inventories.

B. RFID SYSTEM RECOMMENDATIONS

As stated in Chapter II, choosing the right type of system and components is critical in optimizing any RFID architecture. Due to the size of the warehouse facility, the read ranges involved, and the lack of liquid or metal in high concentrations; an Ultra-High Frequency system is recommended. This will provide read ranges of up to 10 meters, making close proximity unnecessary and providing more flexibility in the location and positioning of readers.

Since information transmitted between tag and reader can be observed, it is advantageous to restrict the type and amount of data that travels in this manner. Though security solutions are covered in Chapter 5 of this study, limiting a tag’s response to a simple serial/identification

number which acts as a pointer to a database entry is a simple implementation decision that obviates many of the security concerns. Such a “pointer only” scheme prevents an attacker from gathering any information about the product or its status merely from the number sniffed from the airwaves. The attacker would need to obtain access to the referenced database to glean any potentially sensitive information concerning the tagged item.

This simple response to interrogations reduces the amount of information being transmitted, enhances security and satisfies the requirement to conduct inventories, track product status and location. As a result, it is recommended that cost effective, passive, class 1, Write Once Read Many (WORM) tags utilizing the EPC numbering system be implemented into both the production facilities and the warehouse.

Finally a system will have to be put in place to allow the readers to communicate with the host network to update the database. It is recommended that all fixed reader stations be networked using a wired connection, while portable systems utilize wireless communications such as IEEE 802.11x. Extra security can be achieved by employing secure wireless technology (e.g., WEP, WPA), but the transmission of meaningless serial numbers instead of revealing product information obviates this as an absolute requirement. Security will be covered in depth in Chapter V.

With the frequency, tag type and communication architecture determined, the only remaining question is the actual system design and implementation as it relates to

the current operation of both production facilities and the warehouse.

There are several different factors involved with choosing the optimum system. Perhaps the number one consideration is cost. Tags can cost anywhere from $0.10 to $0.50 depending on capability and number purchased. Since each item must be fixed with a tag, it is probable that initial tag purchases will number in the six figure range regardless of the end state architecture selected.

The number and configuration of the readers required is highly dependent on what the sponsor wants to leverage from the RFID system. As a result, after the recommended system architectures of the printing and tape production facilities are outlined, five different warehouse options are offered for consideration. Each option has its own advantages and disadvantages. In order to quantify the cost of each option relative to the others, a brief cost analysis is offered at the end of each section for comparison.

C. PRINTING AND BINDING FACILITY DIAGRAM

To address the shortcomings of the printing process outlined in Chapter three, RFID has been introduced to automate object tracking and status. As noted in figure 17 below, *“labeling”* TP4 has been replaced on the state transition diagram with the insertion of an RFID tag immediately following the verification process. This decision was made to facilitate a more timely verification process immediately following the printing phase. Following the placement of a tag on the item, the transponder is read and the object added to the database. This allows the

facility manager to henceforth have a positive control over all printed and verified products in the printing facility.

If an item is subsequently identified for disposal due to document error or over-production, the object tracking continues until it is removed from the database by passing through the disposal reader marked “destruction” on the diagram.

The remaining items (not marked for destruction) that continue through the printing process can be tracked and located through a sequence of readers located at the “cut and binding”, “inspection”, “packaging” and “transportation” phases of the printing production process. This allows positive control to be maintained until the product is transported through the exit reader and moved to the warehouse facility. During the “in transit” phase, the object status will be updated as shipped and removed from active status in the printing facility database.

As in the previous Chapter, the following notation is utilized in the diagram below and describes each state and transition that occurs during the printing production phase.

State Printing (SP) – State of a “book” during the printing phase of the production process. Each state is given a title and labeled in a logical, numerical sequence from 1 to n.

Transition Printing (TP) – Transitions of a “book” from one state to the next. Each is given a title describing the transition and labeled in a logical, numerical sequence from 1 to n.

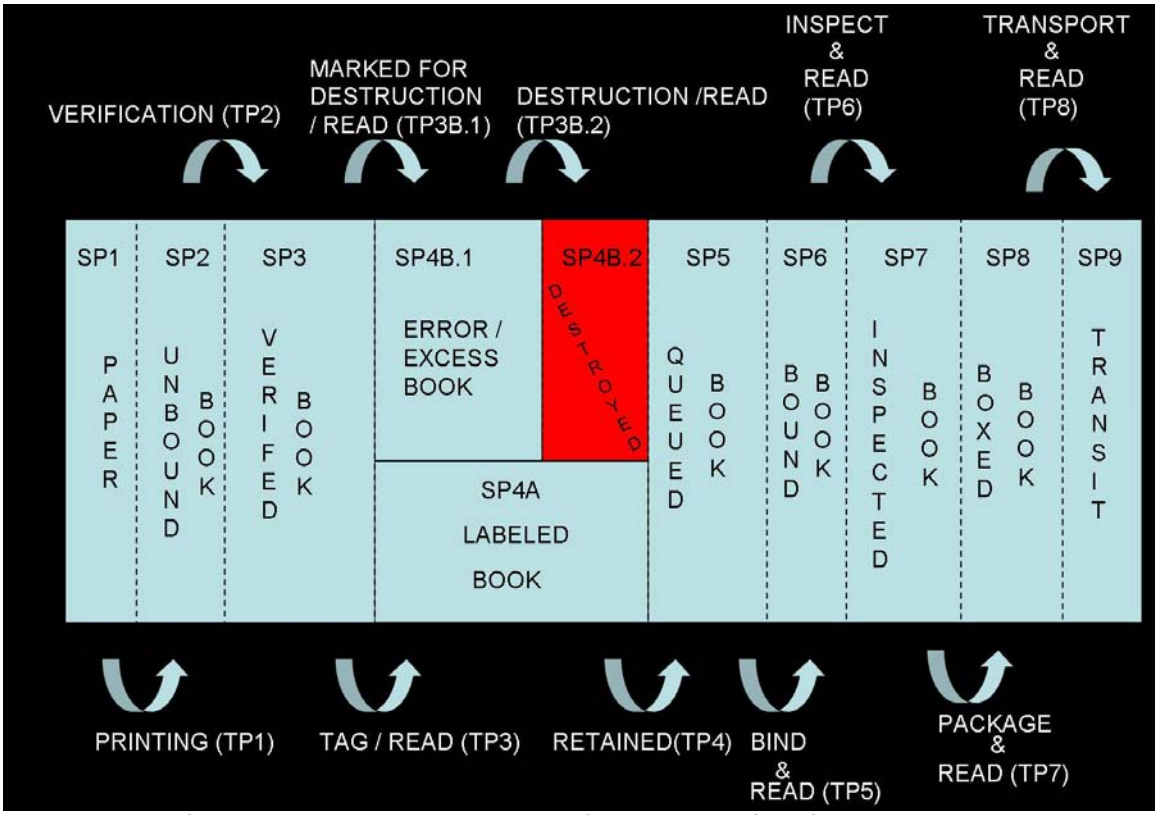

Figure 17. Recommend RFID Printing Process

D. TAP PRODUCTION AREA DIAGRAM

As stated previously, the tape production facility is a more compact and less complex environment when compared to the printing facility; reducing the need for a complex object tracking and inventory system. However, using RFID to replace bar code labeling would facilitate improved tracking during both the production and warehouse phases of the supply chain. During "*transition*" TT4 in figure 18, the bar code labeler is replaced with a mechanism to implant RFID tags. The tags are immediately read and logged into the facility database.

The canisters can then be tracked through the production process until the tag passes through the gateway

reader at the exit and logged as inactive in the tape production facility database.

The following notation is used:

State Tape (ST) – State of a canister/tape during each phase of the punching and loading process. Each state is given a title and labeled in a logical, numerical sequence from 1 to n.

Transition Tape (TT) – Transitions of a canister/tape from one state to the next in the punching and loading process. Each is given a title describing the transition and labeled in a logical, numerical sequence from 1 to n.

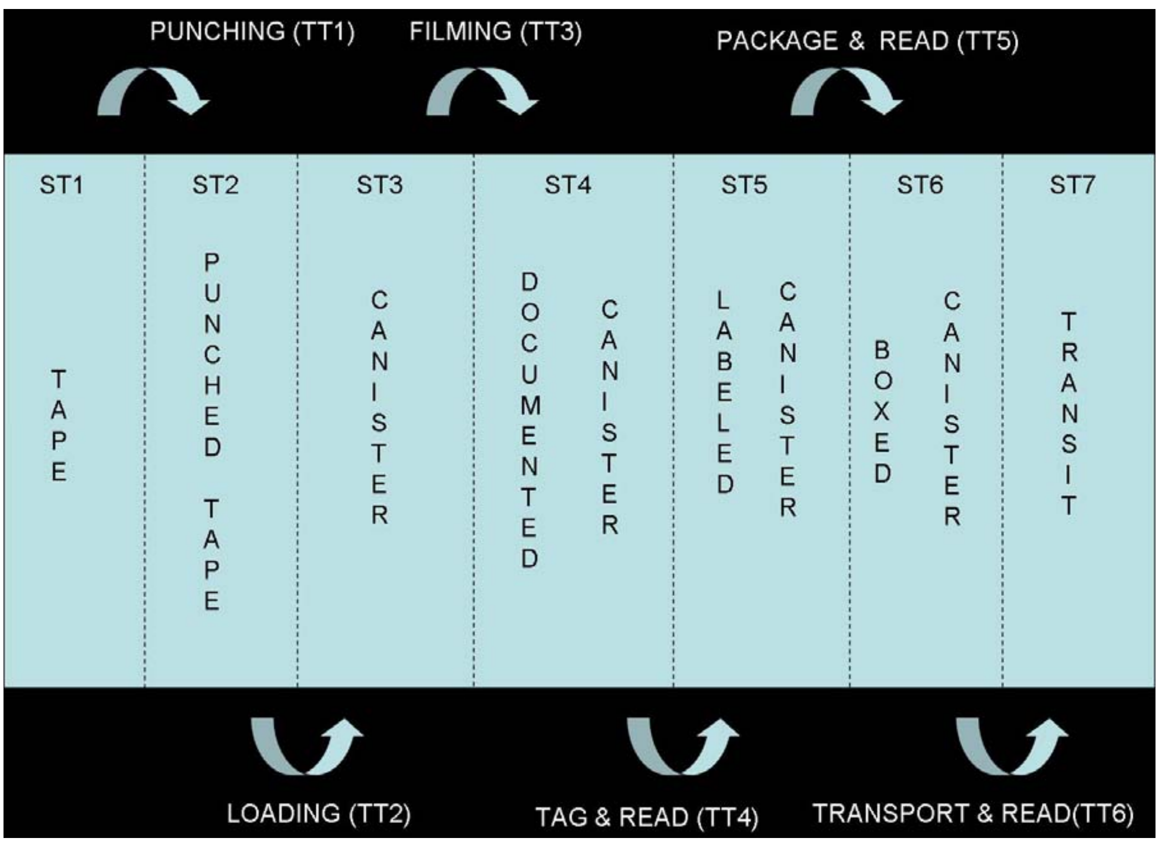

Figure 18. Recommended RFID Punching Process Diagram

E. WAREHOUSE FACILITY

While RFID does add significant value to the printing and marginal value to the tape production facilities, it is in the warehouse that it can be leveraged most to improve inventory awareness. Each of the suggested RFID employment options discussed below provides this enhanced awareness with incrementally more automation, but with the expected increase in cost that such automation entails.

1. Option #1: Archway Readers

This option offers the very simplest in RFID integration and would require placement of three RFID archways, like that displayed in figure 6. One archway located where tagged objects enter the warehouse, one where tagged objects are packaged for customers, and one where the tagged objects exit the warehouse when shipped. As each object enters the facility, it passes through an entrance archway that is networked to a host database system. Each tag is scanned and the product is added to the inventory before it is placed in its storage area to await collection and shipment to the customer.

When required, the items are then gathered in the present fashion using a clipboard manifest and bar code scanner. Following collection, the products are passed through an archway reader where they are checked against an electronic item manifest stored in the host system. Each item that matches the manifest will be updated to reflect its “verified” status before being taken to the packaging area where it will be boxed. If however, excess items are present or the stated manifest requires an item that was not recorded (i.e., not read by the archway reader), the user will be notified of the discrepancy.

Once all verified items have been packaged and boxed, they are placed on a pallet to await shipment. As the pallet exits the warehouse and is put in a truck, the contents of the pallet are read and each item updated to reflect its “shipped” status in the database.

The clear advantage of this option is the small initial investment in RFID and the lack of a wireless infrastructure required to support it. Each of the archway readers can be hardwired into the host network making this the most secure system from a communication perspective. RFID can be leveraged to maintain item presence within the facility, making infrequent inventories less risky. It will also eliminate the time consuming and manpower intensive current practice of inspecting and verifying each item twice following the collection process.

The downside to this option is the lack of a complete tracking and status capability. Because there are only readers located at three critical points within the facility, the warehouse manager only knows that the items are present somewhere in the building. The precise locations cannot be ascertained without conducting a time consuming manual inspection. This manual inventory currently takes weeks to complete, resulting in a situation where an item could be “missing” for up to six months without the knowledge of the facility manager (assuming a bi-annual inventory schedule).

To facilitate this inventory and the collection process, the old bar code system must also be left in place in order to inspect and record each item. Though this may be an excellent intermediate/transition solution for integrating RFID into the supply chain, it is not a

recommended long-term solution as it does little to improve the current inventory process. If, however, the manager desired to have the old system remain in place as a backup while a more capable system was built and tested, this option may provide a cost effective first step worth considering.

The following diagram outlines the state transition diagram describing the simple archway readers RFID option with the following notation:

State Warehouse (SW) – State of a product (book or canister) during each phase of the storage and distribution process. Each state is given a title and labeled in a logical, numerical sequence from 1 to n.

Transition Warehouse (TW) – Transitions of a product from one state to the next in the storage and distribution process. Each is given a title describing the transition and labeled in a logical, numerical sequence from 1 to n.

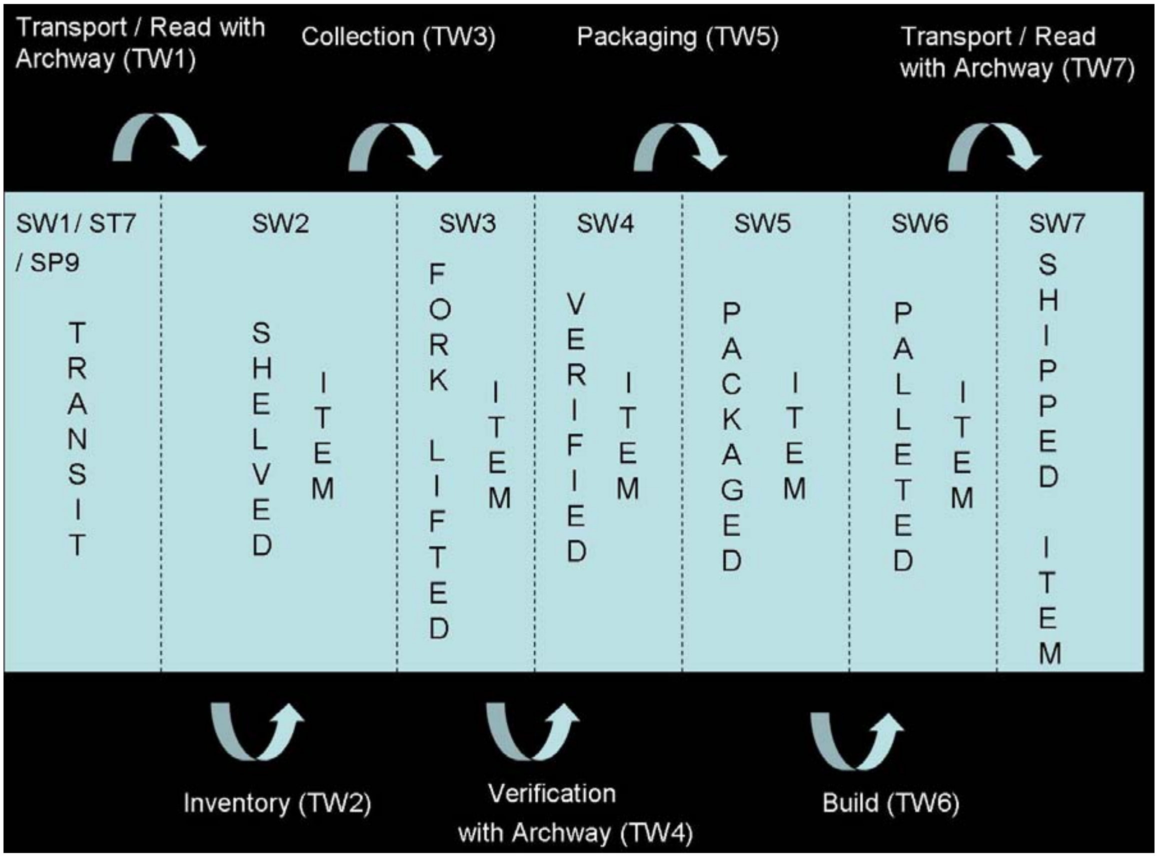

Figure 19. Archway Readers.

Cost Analysis

1,000,000 T1 + 3 RA1

T1 – Passive WORM UHF RFID tag

RA1 – Archway Reader

2. Option #2: Archway Readers/Inventory Handhelds

Option #2 is exactly the same as option #1 with one distinct difference; the use of handheld RFID readers to conduct inventory. During inventory, the tags quickly scanned and the database updated to reflect the presence of each object and its current location (shelf). Because the

line of sight and visual check-off of each object is eliminated, the time to conduct the entire process is reduced drastically, making faster and more frequent inventories possible, and thus reducing the time to discovery of a missing object.

The downside of this option is the need to purchase handheld RFID readers that communicate to, and are integrated with, the object tracking database. This can be done through a wired or wireless system.

The following state transition diagram describes the process with the following notation:

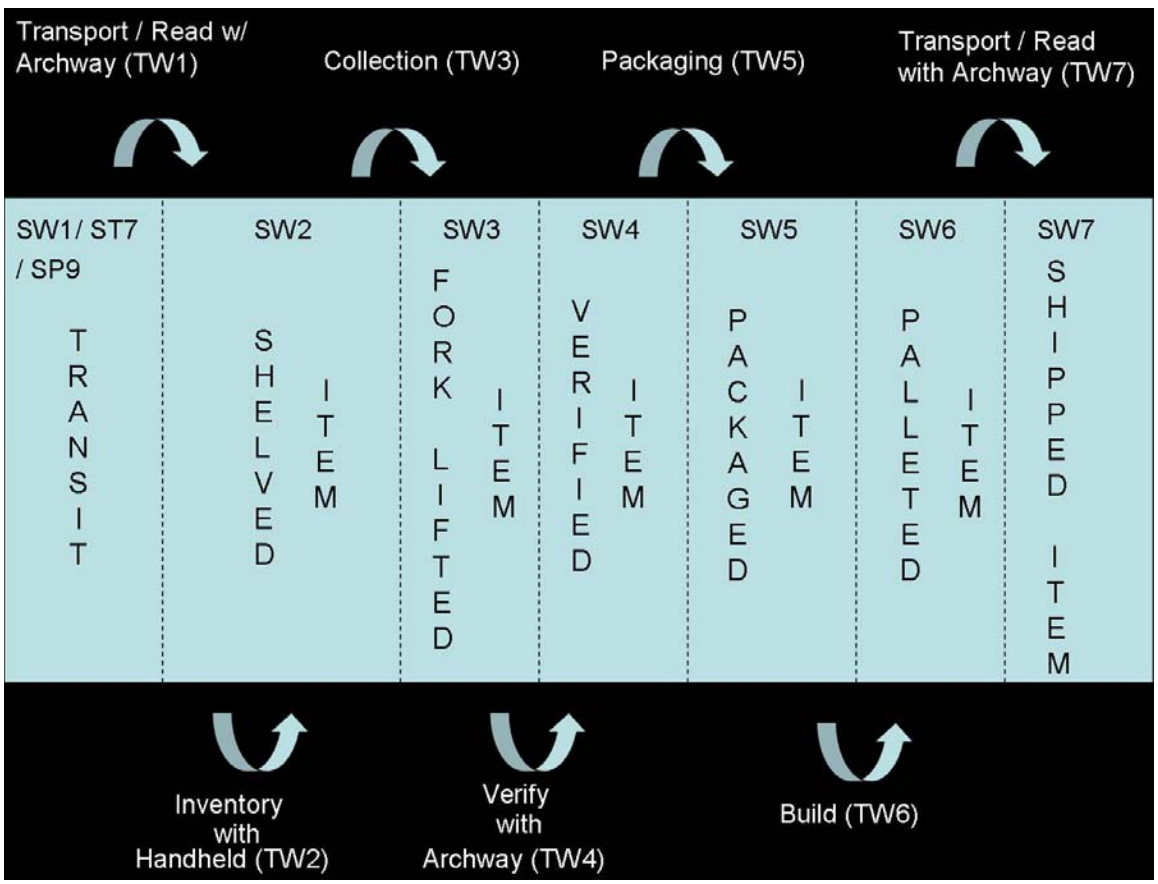

Figure 20. Archway Readers with Handheld Inventory.

Cost Analysis

1,000,000 T1 + 5 RH1 + 3 RA1

T1 – Passive WORM UHF RFID tag

RH1 – Handheld Reader

RA1 – Archway Reader

3. Option #3: SMART Handhelds/Readers Archways

The third option uses the same archway system as outlined in option #1 but with the addition of “SMART” RFID hand readers. These readers would be the focus of the warehouse facility. They would be capable of displaying the manifest of items to be collected by a user to fill a job order. Items would appear on the screen in logical order according to their assigned physical locations on the warehouse floor. The fist item and its location would be displayed for the user to collect.

Once that item’s tag was read as it is removed from its box, the user would receive a visual confirmation on the SMART readers’ display and the items’ status would be immediately updated in the database. Following confirmation of an item’s presence on the electronic manifest, the title and location of the next item to be collected would be displayed. The above process would be repeated until the entire job was collected.

Again, the items would be verified by an archway located at the entrance to the packaging area before finally being logged out by the warehouse exit reader at time of shipment.

The state transition diagram below illustrates the complete process below.

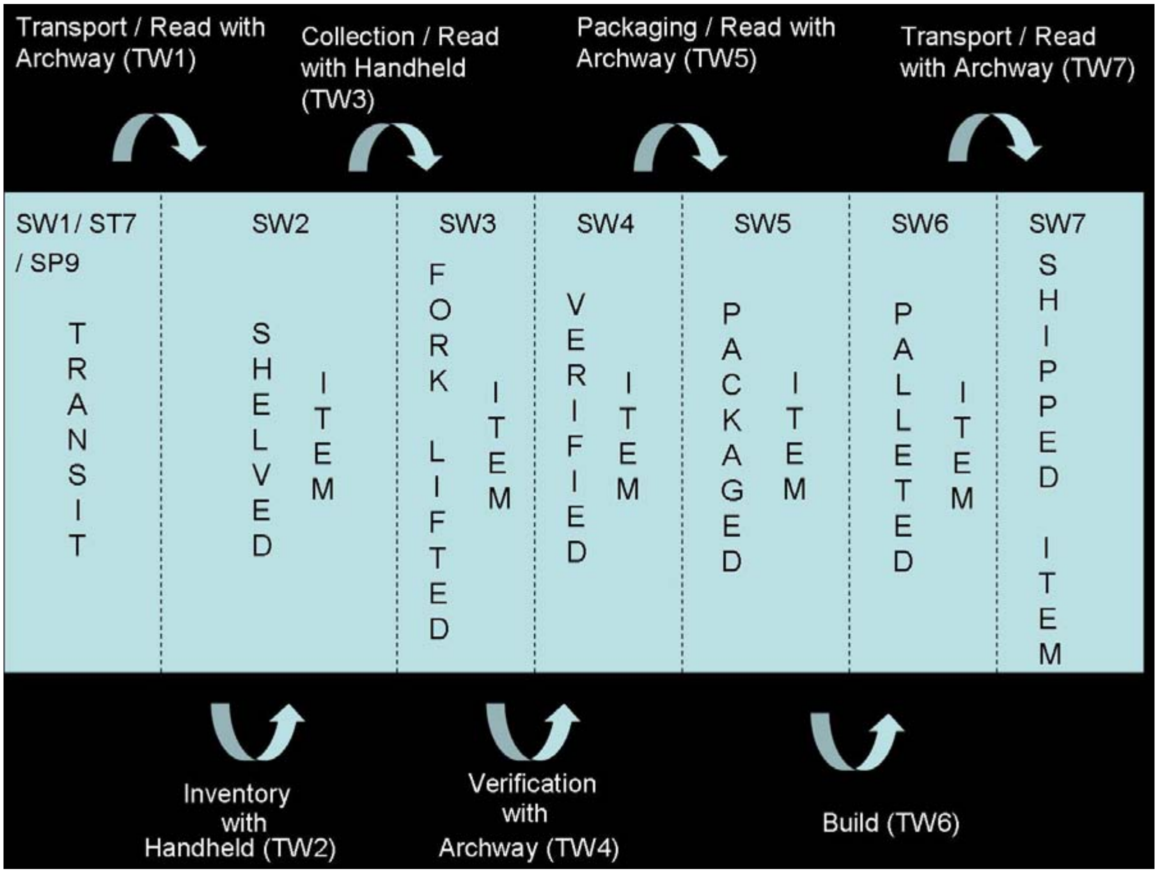

Figure 21. Archway Readers with Smart Handheld Readers.

Cost Analysis

1,000,000 T1 + (10 Increased Cost SMART Reader) x 5 RH1 + 3 RA1 = **1,000,000 T1 + 50 RH1 + 3 RA1**

T1 – Basic UHF RFID tags with WORM capability

RH1 – Handheld Readers

RA1 – Archway Readers

4. Option #4 SMART Shelves

Wal-Mart and Gillette have recently abandoned the attempt to install smart shelves in their retail facilities, citing privacy concerns. They have however begun increasing the level of RFID technology employed in their warehouses [6,7,8]. In a small scale environment where object tracking is of great importance, smart shelf architecture may offer significant benefits.

This option would require the installation of readers on each shelf address to detect the presence of any RFID tag that passes between them. An example shelf reader configuration is shown in figure 22.

Figure 22. SMART Shelf.

Each item that is removed from the shelf would pass between the readers and be logged out of that shelf’s storage location in the database. This option represents a “delta” inventory system. Such a system cannot provide a positive check of inventory, but rather depends on an accurate starting inventory from which it will record

changes (i.e., additions to and deletions from the starting inventory).

An item that is removed from the shelf would be checked against all active manifests to ensure the necessity of its removal. Any unexpected removal of an item from the shelf’s inventory could then be “flagged” and the warehouse manager notified. Of concern is the collision problem described in Chapter II. Tests would have to be conducted to ensure that the readers could distinguish individual tags amidst the potentially large collection of tags during pallet delivery. Current published material suggests that readers can differentiate tags on the order of several hundred per second, but actual performance is vendor, object, and environment dependent [2].

An actual periodic inventory would be conducted using handheld readers as outlined in option #2 to verify the virtual inventory provided by the shelf readers.

Collection could be done with a clipboard manifest without the need for the current bar codes. Again, item manifest verification would occur just prior to the packing stage before the items are read by the warehouse exit reader at time of shipment.

The advantage to this option is the ease of collection, requiring the user to simply remove an item from the shelf to change its status in the database.

The disadvantage is the number of readers that are required to monitor each address location, on the order of roughly 2000 based upon the brief site survey conducted in August of 2005 and as explained below in the cost analysis section.

The process is again outlined in the state transition diagram below.

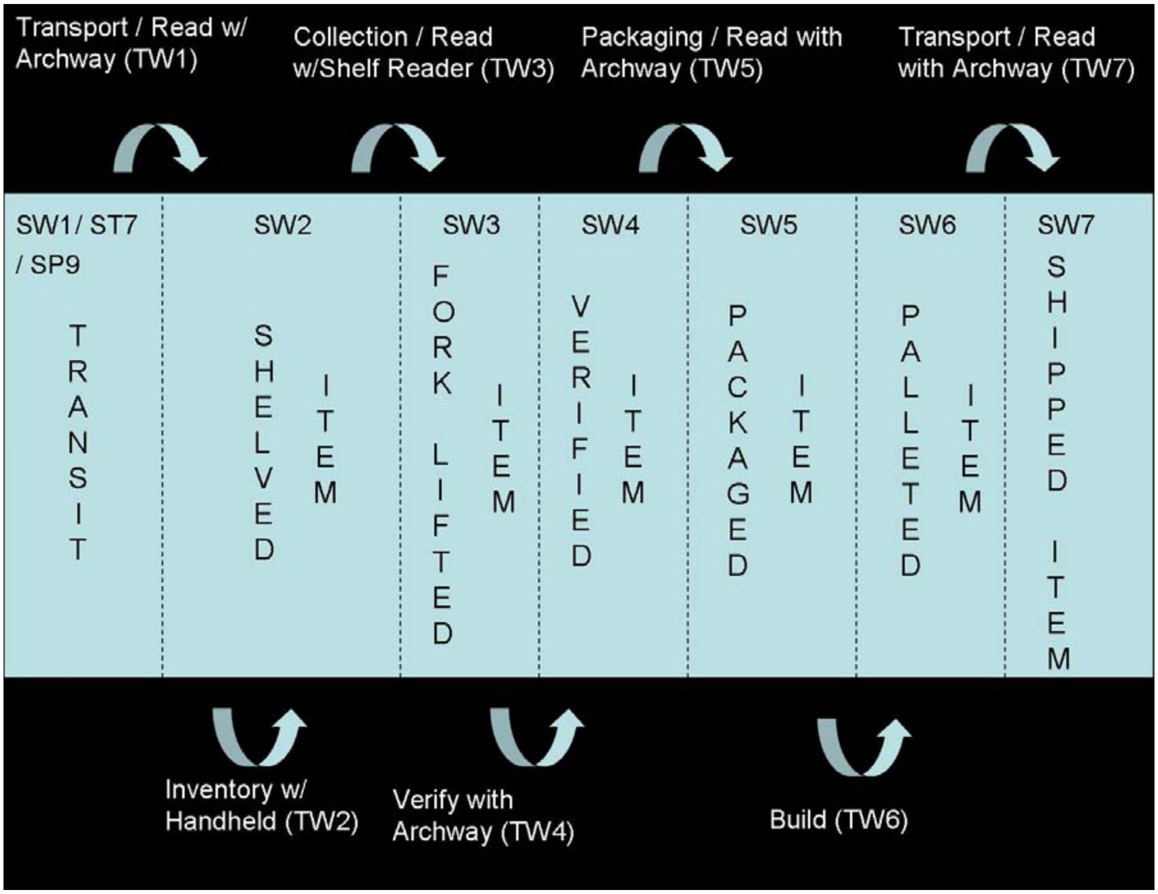

Figure 23. Shelf Readers

Cost Analysis

1,000,000 T1 + (40 Shelf locations per address x 5 levels per address x 12 address) R1 + 5 RH1 + 3 RA1 **= 1,000,000 T1 + 2400 R1 + 5 RH1 + 3 RA1**

T1 – Passive WORM UHF RFID tag

R1 – Shelf Reader

RH1 – Handheld Reader

RA1 – Archway Reader

5. Option #5 Super Bin Readers

The final recommended option for integrating RFID into the warehouse facility involves the capability to read tagged objects in a fully automated fashion while they reside at their individual storage locations (shelves). This would make it possible to conduct fast, complete inventories at set/frequent intervals or as needed in push-button automated fashion; thus vastly improving inventory awareness. However, this added capability will likely be quite expensive relative to the other, less capable options presented so far.

As described in Chapter II, the distance at which RFID tags can be read is limited depending on system design. As a review, some of the most important factors affecting read distance are; transmit power, antenna size, signal attenuation and the tag antenna’s orientation relative to that of the reader. As tag and reader capability increase, so does cost, sometimes exponentially.

The manner in which books are placed in their box will have a significant impact on readability. For example, if the books are stacked lengthwise such as how papers are placed into a filing cabinet, the reader would have to be placed to the side of the pallet. Otherwise, the tags will be orientated ninety degrees off the axis of the reader (i.e., the reader is placed above or below the pallet). This may not allow for sufficient power to penetrate the

many boxes and books to generate a readable response from each tag.

If, however, the books are stacked vertically one upon the other, the reader would be most effective above or below the boxes on the pallet. As stated in Chapter II, the FCC regulates the amount of power that can be transmitted in the unlicensed ISM frequency bands. This limitation may result in insufficient power to read a tag with perhaps as many as thirty thousand pages of paper between it and the reader (assuming a pallet with boxes stacked twelve high, with fifty books per box and fifty pages per book).

There are several possible architectures for providing continuous item level inventory in a RFID enabled facility. Most commercial companies conduct inventories at the box, or even pallet, level due to the high costs of tracking individual items.

An automated inventory can be done in one of four major ways. Centralized, n-tier, distributed, and distributed n-tier. Each has its advantages and disadvantages.

A centralized architecture is designed around a strategically placed “super reader” that could ideally (though theoretically un-feasible) interrogate every tag from a single, central location. Due to the size of the sponsor’s facility and the density of item material, this could only be accomplished by using active RFID tags. Passive tags lack the necessary power to be read at more than 20 meters distance. Since the required distance could be more than 250 meters, a centralized architecture using a passive system is not recommended.

Active systems present their own difficulties. Due to the presence of an onboard power source, active tags are currently too large and bulky to be easily placed on the cover of a book. Further, these tags are anywhere from 20 to 100 times more expensive than their passive counterparts. In a facility with up to 1,000,000 product items, active tags employed at individual item level granularity would be quite costly relative to the other methods discussed.

Using a centralized reader would also exacerbate collision challenges as one reader would be responsible for reading hundreds of thousands of tags. Even with today's complex collision avoidance algorithms, sorting through several hundred thousand responses would be difficult, if possible at all.

Finally there are great security challenges associated with active RFID. The readable distance can be up to several hundred meters. As a result, eavesdroppers could listen to the data exchange from a remote location presenting an obvious security problem if anything other than simple serial numbers are transmitted.

Setting up an n-tier (with n in this example equal to 4) architecture for the sponsors warehouse would require a centralized reader (top tier) to interrogate tags located on pallets (tier 2), which would in turn interrogate boxes (tier 3), which would in turn interrogate books/canisters (tier 4). This requires a combination reader-responder on every box and pallet in the warehouse; which would number in the tens of thousands.

Part of the cost problem of an active RFID system would be solved if the pallets contained active tags with read ranges long enough to communicate with the central reader. However, due to the massive amount of material contained on a pallet, each box would be required to contain a reader making this option cost prohibitive as passive readers can cost a $1000 or more.

A distributed architecture would be realized by placement of a reader at each shelf location to read the contents below it. Each shelf reader would be networked into the RFID reader LAN, which would be shared by the system running the RFID middleware and hosting the inventory database. The issue here is one of physics once again. The FCC restricts the power that a shelf reader can transmit making it very improbable that an EM wave would be able to generate a response from a tag with 30,000 pages of paper between it and the reader where the EM wave originates. One solution is to simply redesign the storage shelves and pallets to reduce the number of boxes each reader must traverse. However, without extensive testing, it is impossible to predict how much material a reader operating at maximum power with ideal coupling conditions, could penetrate.

The final architecture is a distributed n-tier made up of networked shelf readers, as in the previous example, communicating with reader/responders located on the boxes which in turn interrogate the books/canisters they contain. This again would require tens of thousands of reader/responders to account for each box, making the option very costly.

Since none of the above architectures offers an attractive solution, we attempted to present an analysis of

the best architecture with some slight modifications for consideration.

A distributive solution provides perhaps the best solution to conducting an automated inventory because of the short communication ranges between box and the items they contain. However, since readers are expensive and hardly disposable, a reusable storage device such as a bin would be desirable. Bins are larger than boxes and therefore capable of storing more items , thus reducing the number of readers required.

Figure 24. Bin

The process would be as follows; each item would be loaded into a bin at the production facility with the tags orientated so that the bin reader can best interrogate the contents. An example of an RFID bin is shown in the figure 24.

Once the items reached the warehouse, the manager could conduct an interrogation of the bins at any time he

or she chose. In order to facilitate this, a wireless system would be required to communicate with the bins. Once interrogated, each bin would read its contents and report back to the host. This would give the warehouse facility manager the capability to conduct a full warehouse inventory in a very short time (on the order of approximately one minute).

The remaining process can follow that outlined in option #1 since handheld readers are not necessary to perform inventory. As in option #1, the archway readers would read the contents of the pallets as they entered, exited and proceeded through the inspection zone. The collection process could be conducted using a clipboard manifest.

There are several downsides that offset the benefit of an automated inventory system:

1. Empty bins would need to be returned to the production facility and re-used imparting a logistical penalty that may offset or reduce the advantage of an integrated RFID tracking system.
2. Items would have to be placed in the bin so that their tags are orientated to the reader. This could result in a change of current packaging procedures.
3. Each bin would require an on-board power source that would have a finite lifespan and necessitate periodic replacement.

4. Each bin would require its own reader, making this quite costly.

The state transition diagram illustrates the suggested process below with the following notation:

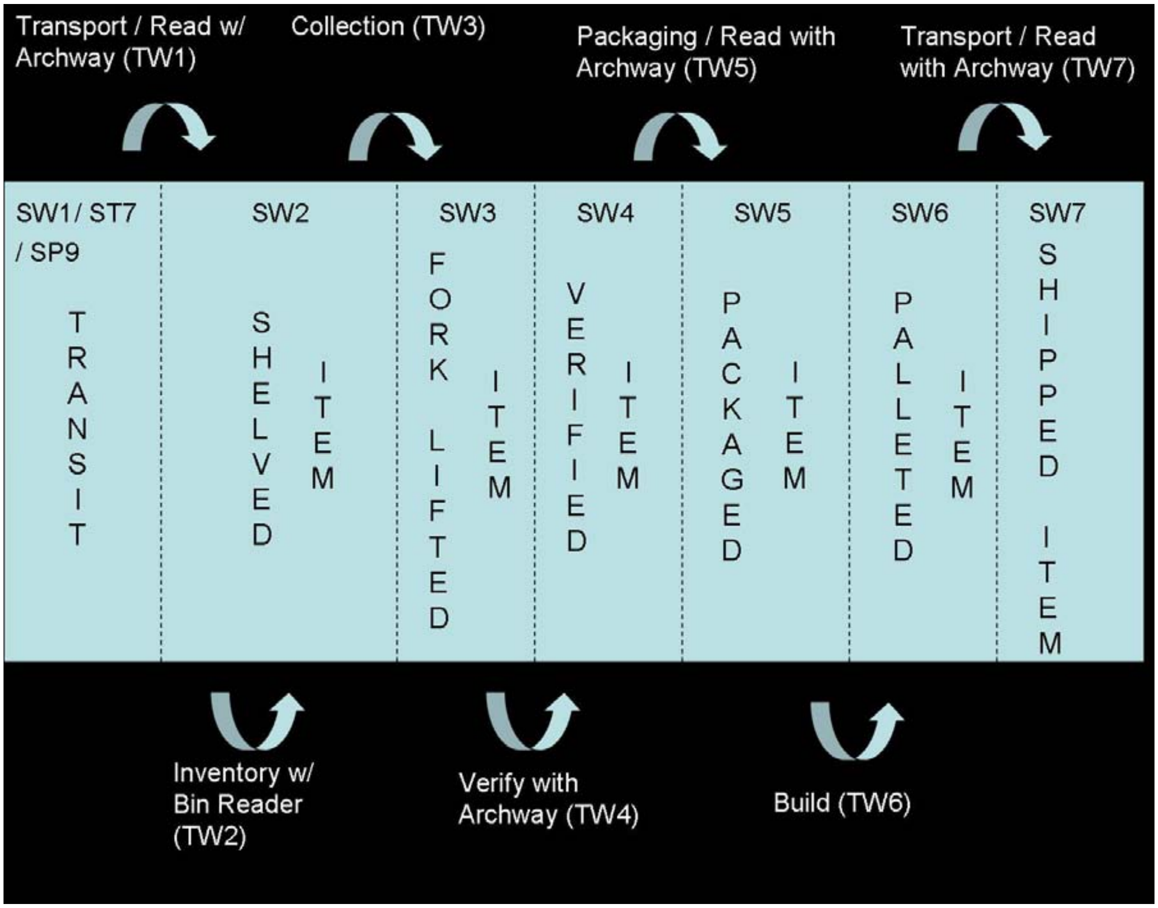

Figure 25. Fully Automated Inventory with Bin Readers

Cost Analysis

1,000,000 T1 + (8 bins per pallet x 80 pallets per shelf address x 5 Levels per shelf x 12 shelf addresses) R1 + 3 RA1 **= 1,000,000 T1 + 38,400 R1 + 3 RA1**

T1 – Passive WORM UHF RFID tag

R1 – Bin Reader

RA1 – Archway Reader

Though an automated inventory capability is of considerable value to a manager maintaining thousands of sensitive items, the cost of such a system is clearly extensive. Many changes would have to be made to the shelving units and the way in which items are packaged. Re-usable bins with limited power supplies will have to be traded back and forth between production facility and warehouse. A secure wireless system must be incorporated adding expense and increasing the risk of information compromise. As a consequence of the above, it is recommended that an extensive cost benefit analysis of such an automated system be conducted prior to implementation.

V. RFID SECURITY

A. INTRODUCTION

After cost, perhaps the most significant question with regard to integrating an RFID system into a secure facility is the overarching security implications. Electromagnetic waves propagate not only to their intended targets but also to anything close enough to receive them. This is of concern to an organization that does not want their products to be tracked by outside entities.

This Chapter will cover the many different aspects of RFID security; outline the many characteristics it shares with basic network and computer security and also the vast differences. It will briefly touch upon the academic research that is being conducted in the area of RFID security, and offer some conclusions that address the specific security needs of the sponsor.

B. SECURITY

The goal of security is the mitigation of risk to an asset; in this case the actual objects and the information contained within the entire RFID system. This system includes the tags, readers, host computer and the network connections used to communicate between them.

Risk to an asset is defined as the product of the asset’s value, any vulnerabilities to that asset, and any threats to that asset. Residual Risk is what is “left over” when safeguards are put in place to protect the asset. This relationship is outlined in the equation below [9].

Residual Risk = (Threat) (Vulnerability) (Asset Value) - Safeguards

If there are no threats, or no vulnerabilities, or the asset is valueless; the risk is determined to be zero. This scenario, however attractive, is unrealistic. For real systems, the risk will always be non-zero. If the safeguards put in place equal the product of the first three variables (i.e., if safeguards = risk), the residual risk is zero. In system security design, reducing the residual risk to an acceptable level is paramount. The questions then becomes, what is an acceptable level?

The first step in determining the answer to the above equation is to quantify expected loss if the system is compromised. This loss is the sum of the products of the probabilities of each potential threat and the expected asset loss due to each threat [9].

In a sensitive environment, this may mean the cost in recovering a stolen object and the production of a replacement since the first has been compromised. This, however, could grow much higher if the loss is discovered after the object has been distributed and utilized. The equation below quantifies expected loss [9]. Note that summation subscript “all t” is shorthand for “all potential threats”. Further, such summation is typically done for a specific period of time; usually one year, which sets the duration over which the “probability” is determined.

$$\textbf{Expected Loss} = \Sigma_{\text{all } t}\,\textbf{(Prob. Threat x Asset Value Threatened)}$$

The return on investment made for security purposes is quantified below[9]. Note that “before” and “after” refer to the application of safeguards.

$$\textbf{ROI} = \frac{\textbf{Expected Loss Before} - \textbf{Expected Loss After} - \textbf{Cost of Safeguards}}{\textbf{Expected Loss Before}}$$

The object of a security system should then be to minimize vulnerabilities, identify (and minimize if possible) threats, quantify asset value, and invest wisely in safeguards that will reduce residual risk to an acceptable level.

Figure 26 illustrates the relationship between the three resulting risk categories (None, Acceptable, Unacceptable) in flowchart form.

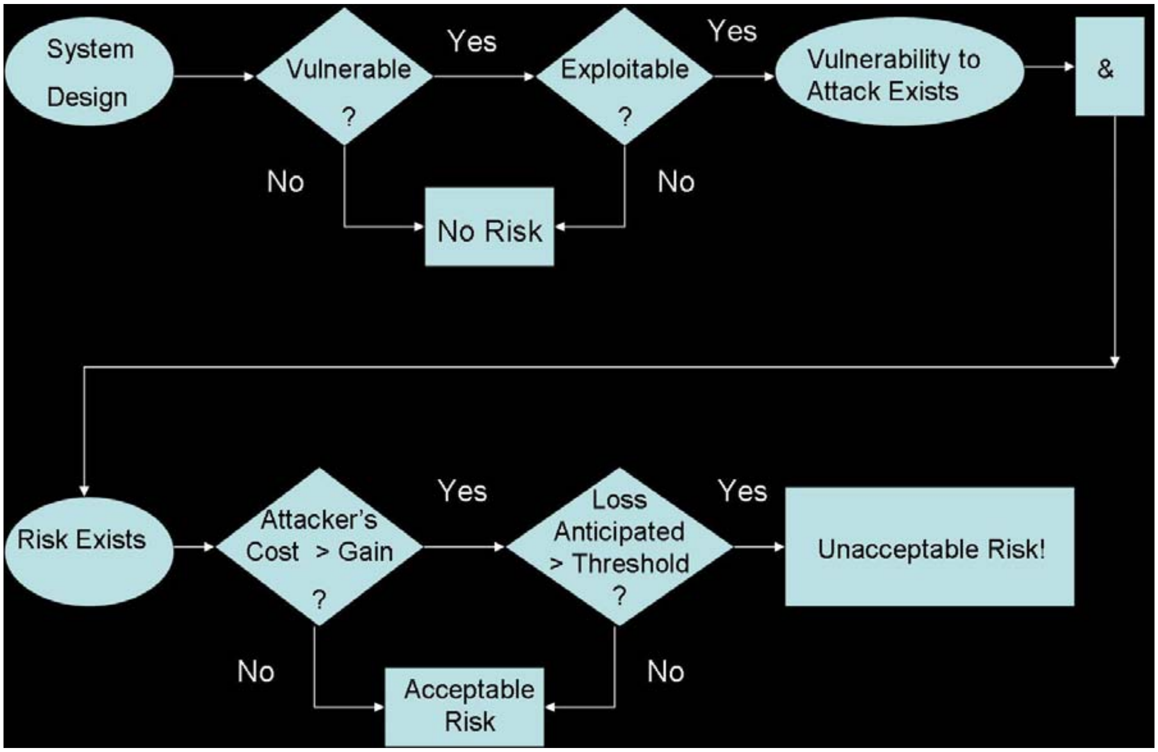

Figure 26. Risk Assessment Flow Chart[9].

C. PRINCIPLES OF SECURITY

In order to understand the principles of security to counter risk, the following taxonomy of security is offered, concentrating on the four main principles, **C**onfidentiality, **I**ntegrity, **A**uthentication and **A**vailability (CIAA):

Confidentiality – Prevention of unauthorized users from observing data.

Confidentiality is achieved through encryption of the data transmitted so that only those with the proper decryption key can observe it. There are two basic types of encryption; symmetric and asymmetric.

In a symmetric system, all trusted users share a secret (synonymous with “key”). The challenge with all symmetric-based cryptographic systems is the secure exchange of the symmetric keys to begin with. That is, a

shared secret is needed in order to share a secret securely.

In an asymmetric system, each user has a public key that is shared with all other users, and a private key that only the user possesses. Data encrypted with a private key can only be decrypted with that key's corresponding (i.e., mathematically related) public key, and vice versa. The challenge in any asymmetric system is the secure and accurate distribution of public keys. This process is resource intensive and difficult to scale for usage among a large community.

Integrity – The general definition of integrity is that information is protected from un-authorized modification, whether such modification is accidental or malicious/intentional. The protection does not require that the information cannot change, but that such a change would be detected if it were to occur.

In order to ensure that a message has not been altered, a one-way algorithm called a hash function is used. Hash functions attempt to transform any given input into a fixed-length, statistically-unique, output that cannot be reversed. In instances where the output is not unique for any two or more unique inputs (a "collision"), it is considered sufficient, in most cases, when these collisions cannot be predicted and are mathematically infeasible to calculate.

To achieve integrity in its most basic form, a message and its corresponding hash value are sent together. The recipient hashes the message received and compares the value with the hash sent with the message. Regardless of

the outcome, the recipient would know if the message was accidentally altered, thus giving integrity. For intentional alterations, where an attacker intercepts the message, changes it, then re-hashes it and forwards the message-hash pair along to the intended recipient; some shared secret would have to be included with the message prior to it being hashed. This is called a MAC (Message Authentication Code). Syntactically, a MAC looks like this: **Message, hash(Message,SharedSecret)**. Note how an attacker would be unable to re-create a new hash without knowledge of the shared secret.

Authenticity – Ensuring that the identity of a user is that which is claimed.

Authenticity cannot be achieved without integrity. A common method to obtain both integrity and authenticity is to use a MAC as described above. This prevents someone who does not have the shared secret from intercepting the message, altering it, hashing the new version and sending it to the recipient.

In an asymmetric system, authenticity is achieved through the use of digital signatures. A message and its hash are encrypted using the sender's private key. The message is then decrypted by the recipient using the sender's public key. The recipient compares the hash of the message to the hash sent. If they match, authenticity and integrity are both achieved.

Availability – Ensuring that information is available in a reasonable amount of time.

The most common way that availability is compromised is through lost or corrupted data, or lost communication;

whether the cause was intentional or accidental. Robust and redundant communications, storage, and processing systems, along with proper resource access control, are the primary safeguards for reducing the risk to availability.

D. SECURITY CONSIDERATIONS

There are several different aspects to consider when developing an effective security plan. The following are areas that should be addressed:

Policy – Managerial policy regarding internal practices and processes with regard to security.

Physical Security – Control physical access to people, materials, and facilities.

Personnel Security – The employment, screening, training and monitoring of personnel in sensitive areas.

System Security – User authentication and access, assignment of privilege. This includes monitoring, log-keeping and auditing.

Network Security – Protecting the network whether wired or wireless, typically through the use of robust authentication protocols, intrusion detection systems, encryption, and firewalls.

E. RFID SECURITY

1. Areas of Vulnerability in RFID Components

Like all data, RFID data is vulnerable to unauthorized access while it is both at rest (i.e., in storage) and in transit. Vulnerabilities in RFID systems can be broken down into four main areas[2].

Tag Data Access – The tag's memory can be accessed through its integrated circuit. This data is vulnerable

when an unauthorized party accesses it, or--in the case of writeable tags--alters it[2].

Tag and Reader Communication – When data is transmitted from tag to reader, it travels via radio waves which propagate to any system in a position to receive them. During this information exchange, the data is vulnerable to observation, interruption, and modification.

Reader Data Access – After the data is collected by the reader, it may be stored by the reader for a period of time, making the data vulnerable to attack while in the reader's memory. [2].

Host Computer System – After transmission of the data to the host, and subsequent storage of the data in the host's database, the host is now an additional target for exposure of any sensitive RFID data. The RFID host is, after all, subject to the same threats as any networked computer [2].

Reader and host threats are beyond the scope of this research.

2. Challenges

RFID security presents a few different challenges that are not present in traditional computer and network security. To begin, all communication done between tag and reader is done through a wireless, EM connection. This means an unauthorized user has the advantage of not having to gain physical access to the network in order to get access to the data. If the information is considered sensitive, it is protected with encryption. If, however, the data is simply an ID number that does not by itself convey any information about the product/object it is

associated with (i.e., it is simply a pointer TO an object's information), its exploitation value is effectively nil so long as the database that maintains the pointed-to information is protected from unauthorized access. This is analogous to finding an automobile's license plate but being unable to cross-reference the plate's number with the DMV's database to obtain information about the car or person it was registered to.

Another significant challenge is tag capability. As expressed earlier, the more capable a tag, the more expensive it is. The additional memory, and logic gates required to perform security functions add a great deal of cost to the tag. A low-cost tag may have approximately 250-1000 logic gates available for security features [10]. Advanced Encryption Standard (AES), a popular commercially available encryption algorithm, typically requires on the order of 20,000-30,000 gates [10]. Even relatively "lightweight" hash functions such as SHA-1 or MD-5 require up to 15,000 devoted logic gates to complete [11]. Adding either of these capabilities to an RFID tag would necessitate a ten-fold increase in processing power, adding significant expense to each chip.

Achieving authenticity with the above resource limitations is another significant challenge. The reader, and by extension the host system, must know that when it receives a serial number response from a tagged item, the item is indeed present and has not been "spoofed" by a fake tag.

In a basic "spoofing" scenario, an attacker could interrogate a tag, then record and write that information to a new tag, and then disable the original tag. The

sensitive item could then be removed from the inventory. This could be done without detection by the host system, which would continue to receive a valid ID response to its interrogations and assume the item was still present.

In order to avoid the spoofing scenario, a tag would have to be authenticated each time it responded to interrogation. This is usually done by having the tag share a secret with the reader (or host system). A tag will “authenticate” by proving that it “knows” this pre-established secret. Using a MAC, the tag would respond to interrogation by the reader by hashing its serial number and the shared secret and sending the result along with its serial number as shown below.

SERIAL NUMBER, Hash(SERIAL NUMBER, SHARED SECRET)

If the reader received a hash other than the one it expected from the tag, it would disregard the response and perhaps respond with an alert to the facility manager.

The biggest challenge with such a transaction is a replay attack. An attacker could interrogate the tag, record the response, and later re-transmit that identical response to the reader, thus “spoofing” a legitimate tag.

To prevent a replay, a tag could use each shared secret only once before discarding it. To authenticate numerous interrogations, the tag would have to store an equal number of shared secrets and be able to communicate to the reader which secret it was using during a given interrogation. Using this protocol, the response would be:

SERIAL NUMBER, Hash(SERIAL NUMBER, SHARED SECRET#5), #5

The reader would insert shared secret number 5 into its hash function and authenticate the tag by computing the same hash value as was sent by the tag.

Though this protocol appears solid, the problem is memory. Currently, class 1 tags do not have the memory to store numerous secrets. Another obvious problem is when the secrets run out, the tag can no longer authenticate itself.

The maintenance of a shared secret is an expensive endeavor. Sharing multiple secrets is even more challenging. The introduction of a nonce (a parameter that varies each time it is used and is never repeated) can eliminate the need for each tag to share numerous secrets with the host system. This could solve both the memory problem and also prevent replay attacks. Each time the tag responds to an interrogation, it would include a nonce as shown below.

SERIAL NUMBER, Hash(SHARED SECRET, NONCE), NONCE

The nonce can be generated by the tag via a pseudorandom number generator or a list of nonces can be maintained in tag memory. The downside of this protocol is the tag resources required. Memory is required to store pre-generated nonces, or alternatively some processing capability is necessary for the tag to generate them. In addition, the reader or host must store each nonce a tag uses for the entire product life span in order to ensure

that it is never repeated. With more than one million tags and perhaps thousands of reads per tag, this would be resource intensive.

3. Research by Academia

"The primary challenge in providing privacy and access control mechanisms in low-cost RFID is scarcity of resources [10]." Sarma, Weis, and Engels suggest in [10] that it will be a significant challenge to the research community to develop hardware efficient cryptographic hash functions for use in low-cost RFID systems. They further suggest that the Tiny Encryption Algorithm (TEA) has a small implementation size relative to AES or Data Encryption Standard (DES), two of the most common encryption standards in use today, and may be a step in the right direction.

To continue this effort, research is being conducted by numerous academics to discover new ways to secure RFID tag to reader communication given their power and processing limitations. It is well understood that tags do not have the processing or memory capacity to perform traditional security functions. Though an entire master thesis could be written summarizing the previous work done in this vein, the following are a few selected summaries that are applicable to the work done in this research.

Sarma, Weism and Engels [12] highlight the limited tag resources as a primary challenge in providing security mechanisms in RFID systems. The authors suggest that new protocols should be developed that low-cost RFID tags can perform. They also cite the problem of tag "spoofing" which would allow an item to be replaced with a cloned tag making it appear that the valid item was still present.

Several academic papers propose lightweight cryptographic primitives for resource constrained applications such as smart cards and sensor networks. Hoffstein, Pipher and Silverman [13], propose a lightweight public-key cryptosystem called NTRU. While what NTRU proposes leads to very efficient mechanisms compared to previously known public-key cryptosystems and digital signature schemes, it still requires resources well beyond what is available on low-cost RFID tags.

Perrig, Canetti and Tygar [14] propose an authentication protocol they call TESLA. It is a broadcast type system for sensor networks which uses symmetric-key cryptography to authenticate. The weakness of TESLA is that it uses hash chains and standard message authentication codes, neither of which can be implemented in low-cost RFID tags. In addition, TESLA requires reader to tag time synchronization, a capability which is also beyond what is feasible in power and processing constrained RFID tags.

Weis, Sarma, Rivest and Engels [15] propose various methods for controlling access to RFID tags. They suggest that a tag can be maintained in two states: locked and unlocked. In the former it responds to all interrogations with only its ID, but in the latter it can perform privileged operations related to security and configuration. The proposed schemes attempt to ensure that the tag enters the unlocked state only if it receives a pre-designated command from a legitimate reader which authenticates to the tag. Again the required authentication protocol goes well beyond the capabilities of a low-cost RFID tag.

Juels [16] attempts to address the problem of privacy protection in low-cost RFID systems. His proposal suggests a scheme where each tag stores a list of pseudonyms. With each interrogation, the tag emits the next pseudonym from its pre-loaded list. Reader to tag query-response rate is deliberately reduced in the protocol, which translates into a slow exchange of pseudonyms. As a result, an attacker can only track a tag if he or she has access to the tag reader communication for a long period of time. The downside of the protocol is that due to their small storage capacity, low-cost tags can maintain only a short list of pseudonyms. Juels attempts to mitigate this problem by refreshing the list with authorized tag readers. Mutual authentication is therefore required between the tag and the reader.

To accomplish this, Juels has developed a lightweight mutual authentication protocol. Encryption is based on a one-time pad. These keys are selected from a series of pads maintained by the tag and updated with new pads in each run of the authentication protocol. Juels' protocol sends the new pads to the tag in the clear, and only allows the new pads to become live after a certain number of updates. This number is high enough that Juels believes that an attacker would be unlikely to have access to the reader to tag communication long enough to observe the specific pad transfer that he could later employ to fake a successful authentication with a spurious tag.

The advantage of Juel's protocol is that it does not require the tag to perform any cryptographic operations other than simple XOR, making it feasible to use in RFID systems. However, updating the pads has a memory cost. In addition, the assumption that an attacker cannot observe

the tag reader communication for a sufficient period is invalid in stationary situations where tags may reside for a significant period of time.

F. SECURITY RECOMMENDATIONS

As stated previously, reader to host communication security and database security are beyond the scope of this study. Of more direct interest to this study is the security of the data contained on the tag and that it is successfully transferred during tag to reader communication.

It is recommended that each tag contain only a serial number which points to relevant information in the database for all tagged items. The exploitation value of this serial number is nearly zero, making the risk of its exposure insignificant so long as the database is afforded sufficient protection using well-established computer security best practices. Therefore, it is unnecessary to protect the confidentiality of the information stored on the tag, or its communication to the reader, using expensive encryption.

The primary security concern is the presence of the tag, or more specifically the item identified by the tag. One of the primary benefits of an RFID tracking system is the ability to track the location of sensitive items. However, in order to achieve authenticity, the host system would have to authenticate each tag. Presently, these authentication protocols are resource intensive and expensive to implement. As demonstrated earlier in the Chapter, each tag would be required to have significantly more memory and/or processing power than is presently available on a low-cost RFID tags.

1. Security Solutions

Though on-tag RFID security mechanisms require extensive tag capability, which exponentially increases costs, it may be possible to mitigate risk through other means not related to tag resources. Some suggested security solutions are outlined below:

Readers at the entrances and exits of the facility – Personnel equipped with RFID ID cards and tagged items could be tracked as they enter and exit an RFID capable premise.

Read Only Tags – Using RO or WORM tags protects data from being rewritten by unauthorized readers.

Limit Range of Communication between Tag and Reader – In most cases increased read range is desirable. However, with regard to security, minimizing read range to that which is necessary for the system to operate is desirable.

Shielding – Enclose the RFID communication area in a Faraday cage. This cage is typically made of steel or aluminum and will reflect EM energy, not allowing it to cross its boundaries.

Though the authentication problem still exists, by incorporating some of the above suggestions, it may be unnecessary to purchase tags that have onboard security mechanisms to reduce risk to an acceptable level. In the risk equation, threats, vulnerabilities and asset value must be compared to the expenditure on safeguards.

In this case, the asset certainly has value, but only within the context of when and where the products are used. If this cannot be predicted, the product is largely worthless.

As demonstrated above, vulnerabilities do exist, but what is the threat? Have those threats already been sufficiently minimized through other security measures to lower residual risk to an acceptable level given the asset value?

Access to the sponsor facility is heavily controlled with all personnel undergoing detailed background investigations and security screenings. This safeguard combined with tags that only respond to interrogations with serial numbers and some of the suggestions above may be sufficient to lower risk to an acceptable level.

Secure RFID communications are not a required element of a security plan. Risk may be maintained at an acceptable level through the use of other security measures as suggested above. It is unlikely that the addition of an RFID system in the production and warehouse facilities will add risk. In fact, more frequent inventories and improved product tracking will likely lower risk when compared to present levels.

Due to the extreme cost, it is infeasible given current RFID technology and the present safeguards in place to invest in a secure RFID system. As chips become more capable it may, in the future, be cost effective to integrate a secure system into the sponsor facility but those conditions do not exist today.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND SUMMARY

This study outlined the current state of RFID technology, giving the reader a basic understanding of the various system components and how they interact. It emphasized the importance of understanding how the physics and components will affect system performance to best leverage the technology when selecting a specific RFID system.

Once the technology was explained, the thesis modeled, in logical form, the sponsor's production and storage facilities using state transition diagrams to demonstrate each phase of the production and warehouse processes. In order to demonstrate where RFID could benefit the sponsor, the diagrams were used again to help the reader understand how and where RFID could be integrated into each facility and what value it might yield. Finally, the challenges and possible solutions to implementing a secure RFID system were explored in Chapter V.

In order to maximize the benefit of employing RFID, the following recommendations were made:

Due to the size of the warehouse facility, the read ranges involved and the lack of liquid or metal in high concentrations, a UHF system was recommended allowing read ranges of up to 10 meters and providing more flexibility in positioning read stations.

It was recommended that cost effective, passive, class 1, Write Once Read Many (WORM) tags utilizing the EPC numbering system be implemented into both the production facilities and the warehouse.

A system will have to be put in place to allow the readers to communicate with the host network to update the database. It was recommended that all fixed reader stations be networked using a wired connection. Readers with write capability will have to be integrated into the production process to assign each tag its serial number.

A. PRINTING PRODUCTION FACILITY RECOMMENDATIONS

Books are currently labeled too late in the printing process to ensure a positive chain of custody throughout the production phase. Labeling should occur immediately after the printing verification phase.

Due to the physical layout of the printing facility, it is necessary to have an automated system to track the status and location of each sensitive item during the production process. This will reduce the possibility that items will be misplaced or improperly removed.

B. TAPE PRODUCTION FACILITY RECOMMENDATIONS

The current tape labeling process should be replaced with a more useful, automation-friendly, RFID tag. Though this may have only a marginal impact on the tape production facility, the product tags can be leveraged during the warehouse process to improve status control, inventory and object tracking.

C. WAREHOUSE FACILITY RECOMMENDATIONS

During the warehousing stage of the supply chain, inventory is currently conducted bi-annually by hand with the necessity for each item to be visually inspected and marked as present. Therefore it is possible for an item to be missing for up to six months before its absence is detected. Inventory should occur far more frequently. An automated process would allow inventory at much more

frequent intervals giving the facility manager confidence in the whereabouts and status of each of the sensitive item.

Following collection, it is currently necessary for each item to be identified and then checked two separate times in two separate locations before packaging and shipment. An automated verification system such as RFID will make it unnecessary for two separate verifications during the collections phase, and reduce the manpower and space these processes currently require.

Five different warehouse RFID options were presented for consideration.

1. Option #1: Archway Readers Only

This option offers a simple RFID solution that would require: one archway to be located where tagged objects enter the warehouse, one where tagged objects are packaged for customers, and one where the tagged objects exit the warehouse when shipped.

Item collection would continue in the present fashion using a clipboard manifest and bar code scanner. Following collection, the products are passed through an archway reader where they are checked against an electronic item manifest stored in the host system.

Once all verified items have been packaged and boxed, they are placed on a pallet to await shipment. As the pallet is driven out of the facility, the contents of the pallet are read and each item updated to reflect its “shipped” status in the database.

The advantage of this option is the small initial investment in RFID and the lack of a wireless infrastructure.

The time consuming and manpower intensive requirement to inspect and verify each item two different times is eliminated.

The downside is the lack of a complete tracking and status capability. Conducting inventories is an issue with this simple system since each item must be accounted for by hand which currently takes weeks.

Option #1 may provide a cost effective first step worth considering.

Cost Analysis

1,000,000 T1 + 3 RA1

2. Option #2: Archway Readers/Inventory Handhelds

Option #2 uses handheld RFID readers to conduct inventory. During the process, the tags are quickly scanned and the database updated to reflect the presence of each object and its current location. Because the line of sight and visual check-off requirements are eliminated, the time to conduct the entire process is reduced drastically, making more frequent inventories possible.

The downside of this option is the need to purchase handheld readers that can record the information received during their interrogations, and upload the data into the database.

Cost Analysis

1,000,000 T1 + 5 RH1 + 3 RA1

3. Option #3 Archways with SMART Readers

This option uses “SMART” readers capable of displaying the manifest of items to be collected. Items would appear on the screen in logical order according to their assigned physical locations on the warehouse floor. The fist item and its location would be displayed for the user to collect. The item’s tag is read as it is removed from its box, and the item’s status updated in the database before the title and location of the next item to be collected would appear.

Cost Analysis

1,000,000 T1 + 50 RH1 + 3 RA1

4. Option #4: Smart Shelf Readers with Archways

The smart shelf system requires the installation of readers on each shelf address to detect the presence of any RFID tag that passes between them. As each item passes through the readers, it would be logged in/out and its status updated as appropriate in the database. This system is meant to start with a known inventory state, which would then be updated as items are added and removed.

Items removed are checked against active manifests to ensure the necessity of its removal. Any unexpected removal could then be noted and the warehouse manager alerted.

Collision problems may occur if the readers are unable to distinguish individual tags in the numbers typically located on a pallet during initial placement of a pallet onto a shelf.

The advantage to this option is the ease of collection, requiring the user to only add/remove an item to/from the shelf to change its status and the virtual inventory that is maintained in real time.

The disadvantage is the number of readers that are required to monitor each address location, estimated at more than 2000 given the current shelf space at the warehouse.

Cost Analysis

1,000,000 T1 + 2,400 R1 + 5 RH1 + 3 RA1

5. Option #5: Bin Readers with Archways

When loading books and tapes at the production facility, it may be necessary to change the way in which boxes are packaged with RFID read capability in mind. Further, since the FCC restricts the transmit power of the reader, it may be necessary to reduce the number of boxes stored on each pallet to reduce the amount of material each reader's signal must penetrate.

There are several possible architectures for providing continuous item level inventory in an RFID enabled facility. While none of the automated architectures offers an ideal solution, a distributive solution provides perhaps a best case scenario where an automated inventory is possible, albeit at great expense. Since readers are

expensive, a reusable storage device is desirable. The use of large bins capable of storing more items than boxes will reduce the number of readers required.

To conduct an automated inventory, a wireless system would be required to communicate with the bins. Once interrogated, each bin would read its contents and report back to the host.

The downsides of this automated inventory capability:

1. Empty bins would need to be returned to the production facility and re-used.
2. Items would have to be placed in the bin so their tags are properly orientated to the reader.
3. Each bin would require an onboard power source that would have a finite lifespan.
4. Each bin would require its own reader, making this by far the most costly of the options presented.

Cost Analysis

1,000,000 T1 + 38,400 R1 + 3 RA1

D. SECURITY RECOMMENDATIONS

Since information transmitted between tag and reader can be observed, it is advantageous to restrict the type and amount of data that travels in this manner. Limiting a tag’s response to a simple serial--number which acts as a pointer to a database--is most logical from a security standpoint. Since each tag should only contain its own serial number, encrypted communication between tag and reader is unnecessary.

To use RFID as an item level secure tracking tool, the reader must be able to authenticate a tag upon interrogation. However, until research matures to a level where low-cost RFID tags can perform protocols like TEA, or hash functions, using fewer logic gates; it will be necessary for a secure chip to have up to 40,000 gates and a few kilobits of memory to process these expensive security protocols.

In order to have long term secure transactions between tag and reader given present technology, it will likely be necessary to employ a chip with some sort of microprocessor, making a semi-passive tag necessary. The chip would also need to be re-writeable to accept new secrets, and have sufficient memory to store them.

Using RFID as a security measure may be infeasible and ineffective when compared to cost. Access to the sponsor facility is heavily controlled. The products themselves are valuable only in the context of when and where they are used. Due to the extreme cost, it may be not be cost effective given current RFID technology and the present safeguards in place, to invest in a RFID system with authentication capability.

E. RECOMMENDATIONS FOR FURTHER RESEARCH

1. A new authentication protocol for low-cost RFID systems could be developed using light-weight algorithms. This would allow each item to be authenticated without a significant increase in cost.

2. Penetration tests of LF, HF, UHF and Microwave EM waves through products normally stored in warehouses could be conducted. This would allow a user to better understand

how to integrate RFID into a storage facility and which system best matched the specific need.

3. Anti-collision solutions must be studied to quantify the conditions under which tags can be read, and at what rate. Since the sponsor desires a system capable of tracking down to the individual item level, anti-collision solutions must be well understood.

4. Research the use of RFID tracking systems to enhance personnel security.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Kleist, A., Chapman, T., Sakai, D., & Jarvis, B. (2004). RFID Labeling – Smart Labeling & Applications for the Consumer Packaged Goods Supply Chain. Irvine, Ca: Printronix.

2. Bhuptani, M. & Moradpour, S. (2005). RFID Field Guide Deploying Radio Frequency Identification. New York, New York: Prentice Hall.

3. Garfinkel, S. & Rosenberg, B. (2006). RFID Applications, Security and Privacy. New York, New York: Addison Wesley.

4. Sweney, J. (2005). RFID for Dummies. Hoboken, NJ: Wiley.

5. Borg, W. (Undated). How to Become An Antenna Guru. Retrieved August, 2005, Website: http://www.borg.com/~warrend/guru.html#pol

6. Roberti, M. (2003). The Shelved Shelf. Retrieved August, 2005, Website: http://www.rfidjournal.com/article/articleview/501/1/21/

7. Dougherty, J. (2003). Technology automatically IDs consumers. Retrieved August, 2005, Website: http://worldnetdaily.com/news/article.asp?ARTICLE_ID=33646

8. Gilbert, A. (2003). Major Retailers to Test 'Smart Shelves'. Retrieved August, 2005, Website: http://news.zdnet.com/2100-9584_22-1023934.htmlhttp://news.zdnet.com/2100-9584_22-979710.html

9. Fulp, J.D. (2005). Course Notes CS3690. NPS: CSR.

10. Sarma, S., Weis, S. & Engels, D. (2003). RFID Systems and Security and Privacy implications. Retrieved August, 2005, Website: http://crypto.csail.mit.edu/~sweis/ches-rfid.pdf

11. Avoine, G. (2003). Privacy Issues in RFID Banknote Protection Schemes. Retrieved August, 2005, Website: http://lasecwww.epfl.ch/~gavoine/download/papers/avoine-cardis-banknote-paper.pdf

12. Sarma, S. Weis, S. & Engels, D. (2003). Radio-Frequency Identifcation: Security Risks and Challenges. *CryptoBytes*, Retrieved August, 2005, Website: http://theory.lcs.mit.edu/~sweis/cbytes-rfid.pdf

13. Hoffstein, J. Pipher, J. and Silverman, J. (2003). NTRU: A Ring Based Public Key Cryptosystem. Retrieved August, 2005, Website: http://whitepapers.silicon.com/0,39024759,60013408p-39000530q,00.htm

14. Perrig, A., Canetti, R., Tygar, J. D. and Song, D. (2002). The TESLA Broadcast Authentication Protocol. Retrieved August, 2005, Website: http://www.ece.cmu.edu/~adrian/projects/tesla-cryptobytes/paper/

15. Weis, S., Sarma, S., Rivest, R. & Engels, D. (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. Retrieved August, 2005, Website: http://theory.lcs.mit.edu/~sweis/spc-rfid.pdf

16. Juels, A. (2004). Minimalist Cryptography for Low-Cost RFID Tags. Retrieved August, 2005, Website: http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/minimalist/Minimalist.pdf

17. Heinrich, C. (2005). RFID and Beyond. Indianapolis, Indiana: Wiley.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Department of Defense
   Attn: David J. Doss
   Fort Meade, MD